



# LOOMING AND OPEN WAR: THE ROLE OF INTELLIGENCE IN A TIME OF SHIFTING GEOPOLITICS

## 2024 SYMPOSIUM REPORT

[www.casis-acers.ca](http://www.casis-acers.ca)  
[casis.substack.com](http://casis.substack.com)

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), the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and the Canadian Security Intelligence Service (CSIS) for their support!



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 Sarah Spence and Nyiri DuCharme

© 2024 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. CASIS symposium attendance is open and includes academics, government officials, lawyers, former intelligence officers, students, and interested public members committed to studying security and intelligence.

## What We Do

For more than 25 years, CASIS has hosted an annual meeting and organized conferences, symposia, and forums focused on intelligence and security topics. The first conference took place at Glendon College in Toronto in June 1984, followed by events in Vancouver, Montreal, Calgary, and Halifax. In recent years, these annual gatherings have been held in Ottawa.

## Subscribe for updates:

[casis.substack.com](https://casis.substack.com)

## Secure Line: A CASIS Podcast

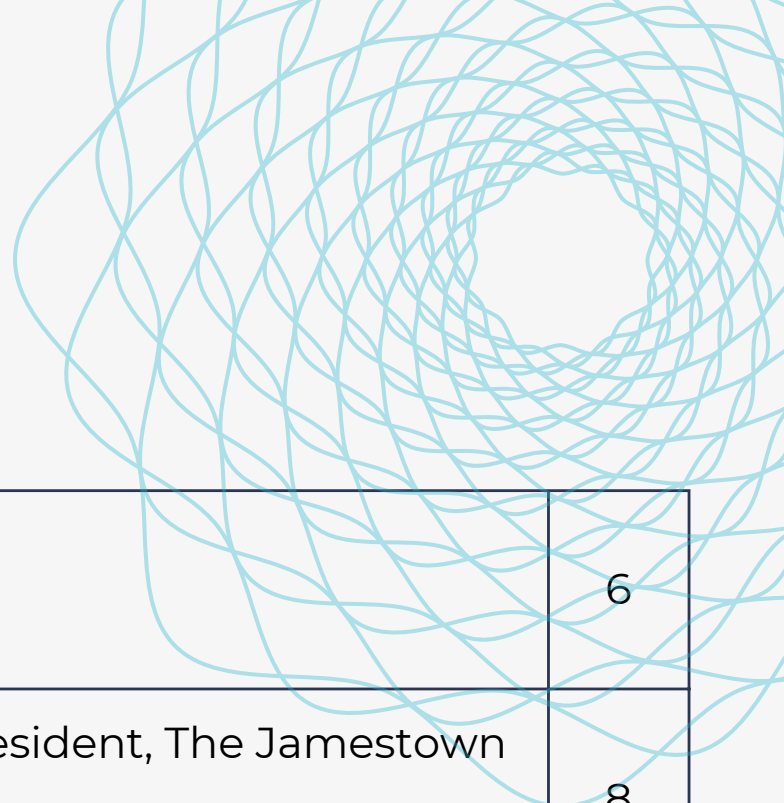
Secure Line is a non-partisan, evidence-based podcast. The podcast aims to influence and inform the debate on security and intelligence in Canada and is hosted by Jessica Davis, Leah West, and Stephanie Carvin.

# LOOMING AND OPEN WAR: THE ROLE OF INTELLIGENCE IN A TIME OF SHIFTING GEOPOLITICS

@CASIS-ACERS

20  
24

# TABLE OF CONTENTS



Executive Summary	6
Keynote Address: Peter Mattis, President, The Jamestown Foundation	8
Panel 1: Intelligence Success, Failure, and Lessons Learned	9
Special Presentation: CASIS Essay Competition Winners	12
Panel 2: The Private Sector Impacts of Shifting Geopolitics	14
Panel 3: Security and Intelligence Cooperation Beyond the Five Eyes	18
Panel 4: The Future of Geopolitics	23




# EXECUTIVE SUMMARY

In his keynote address, Peter Mattis spoke about the importance of governments, intelligence agencies, businesses, and researchers harnessing OSINT, given its value in providing insights into political, economic, security, and social trends. He advocated for creating an OSINT-focused entity that works alongside government to support intelligence functions, leveraging open-source and classified intelligence. Governments are underutilizing open-source information and need to better integrate it into the broader intelligence context.

The first panel focused on how intelligence successes are often built on learning from past failures, which help shape decision-makers' thinking when addressing future challenges. Panelists Emily Harding, Dr. Thomas Juneau, and Michelle Tessier shared their insights, noting that key successes in intelligence are typically the result of timely, accurate, and well-coordinated efforts to gather and analyze information, which enable informed decision-making and proactive actions to safeguard national interests. However, failures arise from gaps in communication, misinterpretation of data, or underestimation of adversarial threats, highlighting the need for constant adaptation and innovation in intelligence operations.

The CASIS-CSIS National Essay Prize Winners presented their papers. Graduate students Aidan Kerr and Nikhil Goyal presented their essay entitled "International Assassinations and Future Research: Insights from the Assassination of Hardeep Singh Nijjar". Undergraduate student Anna Lysenko presented her essay entitled "Eyes Everywhere, Against All Enemies: Analyzing Non-Governmental Open-Source Intelligence in the Russo-Ukrainian War".

*cont'd...*



During the following panel, Peter Elliot, Angela Lewis, and Dave McMahon explored how shifting geopolitical dynamics affect the private sector, particularly in industries with global operations or supply chains. Companies are enhancing their intelligence analysis capabilities to better anticipate, assess, and manage corporate risk. As instability increases, businesses face heightened vulnerabilities, including disruptions to global supply chains, cyber threats, and regulatory challenges.

Jonathan Berkshire-Miller, Dr. Stephanie Carvin, and Vincent Rigby discussed the “Five Eyes” security and intelligence alliance and whether the complex security environment warrants expanding partnerships beyond the “Five Eyes.” The panel speaks about the opportunities for Canada to deepen its cooperation and broaden alliances with countries well-placed to address the evolving security landscape and how diversified alliances could also help strengthen the Five Eyes alliance.

During the final panel, Dr. Simon Miles, Dr. Emily Whalen, and Dr. Joseph Torigian focused on the strategic competition between major global powers, exploring how traditional statecraft evolves and new forms of conflict emerge. Panelists discussed the erosion of liberal values, the rise of authoritarianism, and the changing nature of international relations in an increasingly multipolar world.

Overall, the conference underscored the critical role that intelligence plays in navigating a rapidly changing geopolitical landscape. With increasing complexity and unpredictability in global politics, intelligence remains essential for national security, private-sector risk management, and international cooperation. It will be important to continuously evolve intelligence practices, maintain sound policies and governance frameworks, and collaborate across sectors to address emerging global challenges.



# KEYNOTE ADDRESS

## Peter Mattis

**President, the Jamestown Foundation**

Peter Mattis spoke about the importance of harnessing OSINT and creating an entity that works alongside government to support its intelligence functions. He sees OSINT – the collection, analysis, and exploitation of publicly available information to support intelligence and decision-making processes – as a valuable tool for governments, intelligence agencies, businesses, and researchers, as it helps them gain insights into political, economic, security, and social trends. It differs from classified intelligence in that it does not have to be gathered through covert methods.

Mattis emphasizes that to leverage open-source data effectively, the U.S. needs to establish a dedicated entity with a national mission to collect, analyze, and disseminate open- and commercial-source information. This proposed entity should be integrated into the intelligence community and be capable of collaborating with external partners while ensuring compliance with privacy laws. It would complement existing intelligence efforts, helping to bridge the gap between traditional classified intelligence and the vast amounts of publicly available data that could offer insights into, for example, Chinese statecraft, military activities, and foreign influence operations.

It has become critical to harness all the capabilities of OSINT in intelligence efforts beyond current use. Given the accessibility of OSINT and its ability to provide real-time or near-real-time insights, OSINT – especially when communicated effectively – is a crucial tool for decision-makers.



# Panel 1: Intelligence Success, Failure, and Lessons Learned



## **Emily Harding**

Director, Intelligence, National Security, and Technology Program and Deputy Director, International Security Program at the Center for Strategic and International Studies (CSIS)

## **Michelle Tessier**

Senior Fellow, University of Ottawa and former Deputy Director for Operations at the Canadian Security Intelligence Service (CSIS)

## **Dr. Thomas Juneau**

Assistant Professor, University of Ottawa

## **Moderated by Dr. Jessica Davis**

President and principal consultant at Insight Threat Intelligence and President of the Canadian Association for Security and Intelligence Studies (CASIS)

This panel discussed intelligence successes and how they often stem from timely, accurate, and well-coordinated efforts to gather and analyze information. This enables informed decision-making and proactive actions that safeguard national interests.

Failures typically occur when there are gaps in communication, misinterpretation of data, or underestimation of adversarial threats, underscoring the importance of continual adjustment and innovation.

The key lessons learned emphasize the need for robust intelligence-sharing across organizations, investment in new technologies, flexibility in strategy, and an understanding that intelligence operations must constantly evolve to meet emerging challenges and threats.

Emily Harding centers her views around three key themes: technological adaptability and innovation, effective collaboration and intelligence-sharing, and evolving intelligence techniques to keep pace with threats. Successes have often been rooted in technological integration and strategic partnerships, while failures often trace back to the challenges of adapting to new forms of conflict, such as cyberwarfare and disinformation.

In Harding's view, continuous adaptation, preserving the role of human analysis, and balancing security and ethical considerations are the key lessons learned. She underscores the importance of intelligence practitioners striking the right balance between emphasizing the credibility and key judgements of intelligence for decision-makers, without biasing the decision they make.



Michelle Tessier underscores the critical feedback loop between those collecting intelligence, those analyzing and assessing it, and those using it to make decisions. One of the most significant shortcomings for Canada has been the coordination challenges around integrating intelligence gathered and assessed across agencies into one cohesive voice. Intelligence is central to understanding emerging global trends, anticipating adversaries' moves, and providing governments with the tools to safeguard national interests. It is often about shaping decisions before events unfold and ensuring the security of citizens through both covert and open-source means. Collecting intelligence in line with decision-makers' priorities begins with that feedback loop.

Dr. Thomas Juneau highlights recent successes in intelligence, including the breadth of public engagement in national security. However, this comes with challenges, as more accessibility and outreach by an intelligence agency can bring about a sense of mistrust among the public, making it a double-edged sword. While transparency and open communication are essential to maintaining trust, the nature of intelligence work often makes it difficult to achieve both security and openness. The public might view the engagement of intelligence organizations as a potential source of overreach, manipulation, or control. Public mistrust in institutions is growing, making our society increasingly susceptible to disinformation campaigns. The shortcomings of Canada's access to information regime reinforces the public mistrust and do not help society protect itself from mis- and disinformation.

Accordingly, Juneau is optimistic that review and oversight entities will help reinforce accountability. The lessons that have been learned and continue to be capitalized on are that engagement and transparency require investments in time and resources and must be managed well.



# CASIS-CSIS National Essay Competition Presentations

Moderated by Micah Clark, Founder & Managing Director, Decision Space

**GRADUATE WINNERS: AIDAN KERR AND NIKHIL GOYAL  
(UNIVERSITY OF TORONTO)**

**“INTERNATIONAL ASSASSINATIONS AND FUTURE  
RESEARCH: INSIGHTS FROM THE ASSASSINATION OF  
HARDEEP SINGH NIJJAR”**

On June 18, 2023, Canadian citizen Hardeep Singh Nijjar was assassinated outside a Gurdwara in Surrey, British Columbia. A vocal supporter of the Khalistan movement, Nijjar had been labeled a terrorist by the Government of India. His killing sparked a diplomatic crisis between Canada and India, fueled by suspicions of involvement by the Indian government. Tensions escalated after a similar plot against U.S.-Canadian citizen Gurwant Singh Pannun was uncovered, leading to visa bans, severed economic ties, and a broader international debate on state sovereignty, minority rights, and transnational repression.

Kerr and Goyal note that current IR literature, focused on norms, legality, human rights, and rational decision-making, falls short in explaining such events. Instead, they propose a research approach emphasizing signalling, leadership, domestic politics, and transnational repression. These factors, though niche, provide valuable insights and offer a more comprehensive understanding of international assassinations in the IR context. Rather than offering conclusions or theories on the role of governments or interest groups, they provide competing explanations and perspectives, drawing from media, diplomacy, and informal discussions of the event.

## **UNDERGRADUATE WINNER: ANNA LYSENKO (UNIVERSITY OF TORONTO)**

### **“EYES EVERYWHERE, ALL AGAINST ENEMIES: ANALYZING NON-GOVERNMENTAL OPEN-SOURCE INTELLIGENCE’S (NGOSINT) VALUE FOR UKRAINE IN THE 2022 RUSSO-UKRAINIAN WAR (RUW)”**

During the Russo-Ukrainian War, civilians have become intelligence agents by using technology to amass digital Non-Governmental Open-Source Intelligence (NGOSINT), which the author conceptualizes as raw information produced and shared by Ukrainian non-combatants on social media platforms, including Telegram and X (formerly Twitter).

The paper presents how NGOSINT contributes to Ukraine's resistance to Russia's 2022 invasion. Lysenko presents a dual thesis after qualitative analysis of primary and secondary sources, highlighting case studies from Kyiv, Bucha, and Mariupol between February and April of 2022. First, NGOSINT supported Ukraine's military resistance by giving the Ukrainian army insight into real-time troop movements and targets, which was valuable for military strategy. Second, NGOSINT was vital for Ukraine to document Russian war crimes, with shared footage garnering international solidarity.

Combining the two arguments, the author concludes that in those case studies, NGOSINT was crucial to dissipating the fog of war and establishing Ukraine's domestic and global conflict narrative: that it was defending its sovereignty against ruthless invaders.



# Panel 2: The Private Sector Impacts of Shifting Geopolitics

## **Peter Elliot**

Vice President of Information Security Risk & Compliance, Magna International

## **Angela Lewis**

Head of Global Intelligence, Investigations, and Threat Management  
Creative Artists Agency and Adjunct Professor, Georgetown University and  
the University of Cincinnati

## **Dave McMahon**

Chief Intelligence Officer, Sapper Labs Group Inc.

## **Moderated by Robert (Bob) Gordon**

Executive Director of the Canadian Cyber Threat Exchange (CCTX) and  
CISIS board member

Strategic competition between major powers has shifted how the global security environment is perceived and the environment in which it is executed, as it is no longer the sole domain of nation-states.

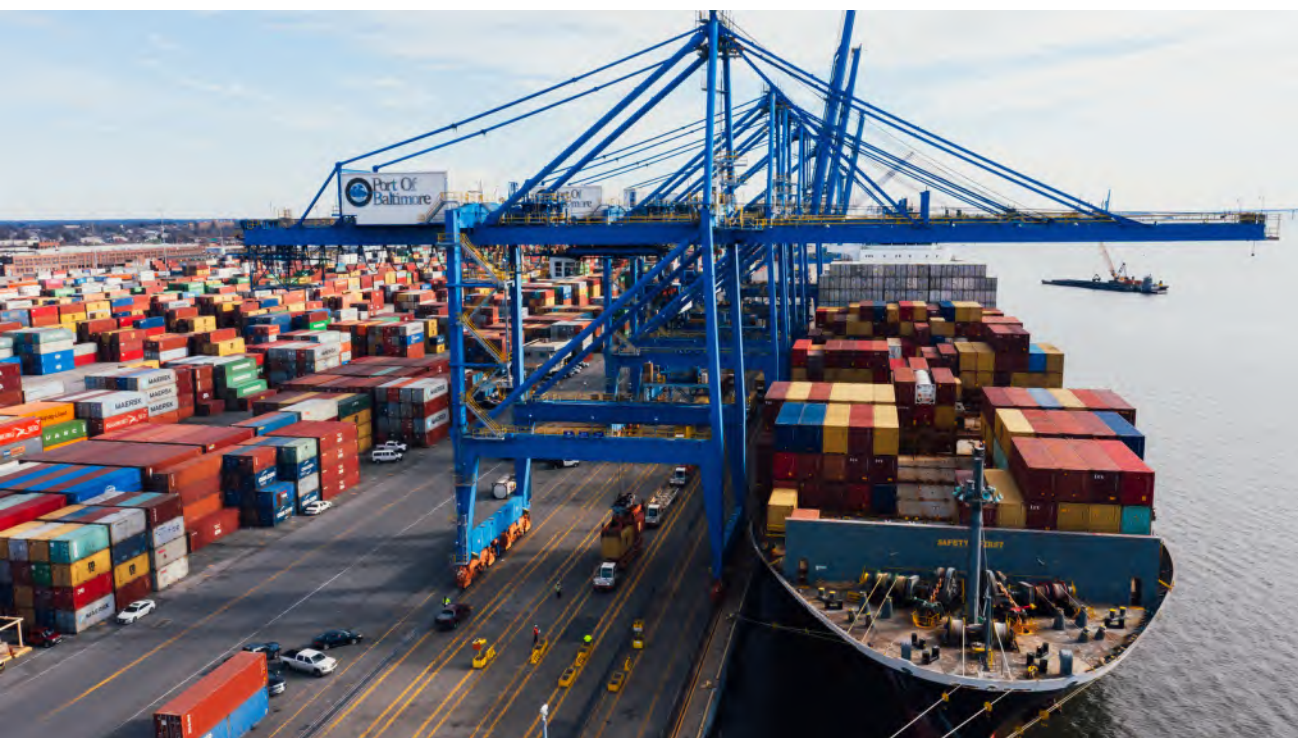
Increasingly, businesses, particularly those with overseas operations, have developed intelligence analysis capabilities to inform decision-making on corporate risk.



Peter Elliot spoke about the opportunities and challenges in cybersecurity. Multinational corporations must be vigilant about securing critical infrastructure and sensitive data, which are increasingly targets for adversarial actors, whether state-aligned or not. Geopolitical shifts, such as trade wars, sanctions, and military tensions, can significantly impact global supply chains.

Over the years, risk compliance has changed – it requires evolving ways of looking for threats and expanding liaison with law enforcement and intelligence agencies. It requires an awareness of trade restrictions, the imposition of sanctions, and other symptoms of increasing conflict that can lead to increased costs, delays, and vulnerabilities – especially for companies with manufacturing plants or other elements of their supply chains in places like Russia and China. These companies can become exposed to significant risks—ranging from geopolitical instability, supply chain disruptions, and loss of market access, to legal and compliance challenges.

Furthermore, Western-based companies with some elements of their operations in more hostile environments can quickly become symbolic targets for cyberattacks and data theft. As global tensions evolve, companies operating in these regions must carefully assess their risk exposure and consider strategies to mitigate vulnerabilities.





Angela Lewis discussed the various risks and challenges she faces while managing high-profile clients, particularly those in the entertainment, media, and sports industries. The threat of data breaches and cyber espionage is a major concern, as is understanding how sanctions, visa restrictions, and shifts in trade agreements can directly impact these clients. Protecting sensitive client data, intellectual property, and financial information requires robust cybersecurity measures.

As a result, proactive threat intelligence, crisis management, and compliance with changing regulations are crucial to navigating the volatile global landscape. Lewis emphasizes the importance of a feedback loop in this process. She explains that business leaders must communicate their specific challenges and concerns so that intelligence briefers can tailor their insights to address them directly. Effective collaboration between the private and public sectors requires clear communication and a mutual understanding of how intelligence can be leveraged to solve complex problems.





As the landscape evolves, more innovation is expected from both sectors. While the private sector has had to be more resourceful in gathering intelligence—often relying on less sophisticated tools and fewer OSINT sources—there is growing support from public institutions that are expanding their role in assisting private sector efforts. In this way, the public sector can play a key role in helping businesses navigate risk and compliance challenges by providing valuable intelligence resources. In sectors where personal safety, public image, and international mobility are critical, understanding and addressing geopolitical risks are essential to maintaining operations and safeguarding stakeholders.

David McMahon spoke about how shifting geopolitical dynamics, such as rising tensions between global powers, directly affect the private sector's cybersecurity position. Nation-state actors are increasingly engaging in cyber warfare or cyber espionage, and these threats disrupt businesses, steal intellectual property, or compromise sensitive data. Businesses that operate in these sectors are at heightened risk of attacks from geopolitical adversaries who may aim to destabilize economies or societies. Accordingly, companies must actively monitor the evolving threat landscape, including cyber threats, terrorism, and geopolitical shifts. McMahon further advises that these companies should be proactive in risk analysis and have a strong intelligence capability to stay ahead of potential threats, both physical and digital.





## **Panel 3: Security and Intelligence Cooperation Beyond the Five Eyes**

### **Jonathan Berkshire Miller**

Senior Fellow and Director, Macdonald Laurier Institute

### **Stephanie Carvin**

Assistant Professor, Carleton University

### **Vincent Rigby**

Ken Slater Professor of Practice at the Max Bell School of Public Policy, McGill University, and former National Security and Intelligence Advisor to the Prime Minister

### **Moderated by Akshay Singh**

Director of Research Security, University of British Columbia and Director of Finance for CASIS

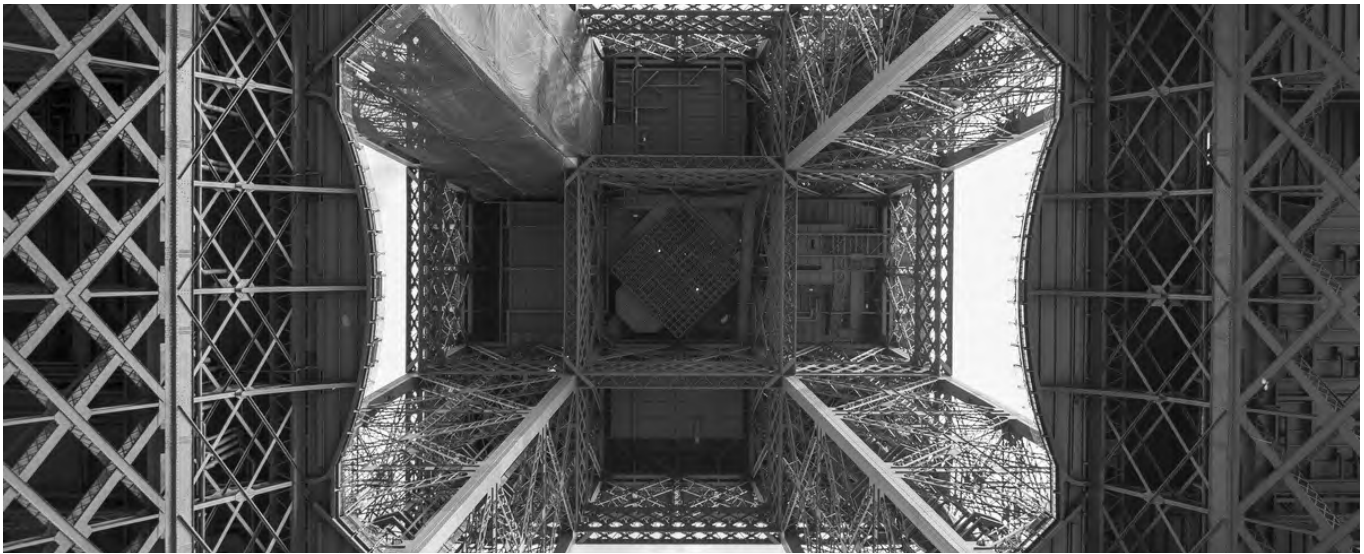
As the world deals with increasingly complex security challenges across geographical regions, it is worthwhile to consider how Canada can cooperate and engage with counterparts beyond its traditional “Five Eyes” partners: the United States, United Kingdom, Australia, and New Zealand.

In 2024, the Five Eyes intelligence-sharing alliance remains crucial to its member nations' security and geopolitical strategies. While the alliance faces significant threats, particularly related to geopolitical tensions with China and Russia, cybersecurity threats, and domestic political divisions—there are also substantial opportunities for deepening cooperation. By focusing on cybersecurity, AI-enhanced intelligence gathering, legal frameworks for data sharing, and expanding alliances with other global partners, the Five Eyes can adapt and diversify their alliance to meet the demands of a rapidly changing world.

Jonathan Berkshire Miller discusses how China's rise and Russia's resurgence are reshaping the global security environment, necessitating broader intelligence and security cooperation beyond the Five Eyes framework. As power becomes more multipolar, with regional powers like India, Japan, and South Korea playing a more significant role, Miller suggests the need for the Five Eyes to engage more with these countries in intelligence sharing and security operations.

The Indo-Pacific Strategy is the first attempt in many years to set Canadian foreign policy priorities, which point toward the partners with whom Canada should work more closely. He also emphasizes the importance of Canada fully understanding the alliances it participates in and the motivations for maintaining them. He asserts that Canada must deliberately define its objectives and expectations from these partnerships. He argues that Canada's defence capabilities must evolve in response to emerging global challenges. In this context, "re-arming Canada" goes beyond merely increasing military spending; it involves investing in new capabilities that are aligned with the strategic realities of the 21st century.

Historically, Canada has focused on peacekeeping and humanitarian missions. Still, Miller argues that, in the face of rising geopolitical tensions, Canada must enhance its military's ability to project power, contribute to NATO defence efforts, and respond to more complex threats, including cyber warfare, hybrid warfare, and great power competition. He asserts that Canada's military readiness needs to align with the demands of modern defence, including the ability to engage in conventional and unconventional warfare.



Stephanie Carvin emphasizes intelligence as a tool of diplomacy. She recognizes that intelligence is critical in shaping diplomatic relations and can be used as both a tool and a leverage point. Her approach focuses on building multilateral intelligence frameworks that are transparent, ethical, and accountable, ensuring that new partners meet rigorous standards of cooperation while safeguarding civil liberties.

In the Canadian context, Carvin acknowledges the perceptions of Canada's contributions to the Five Eyes and being a net "importer" of intelligence; however, she notes that Canada is a much stronger partner than is perceived and leads in specific niche capabilities. For example, the Communications Security Establishment is a leading cyber agency in the world, noted most recently by the UK National Cyber Security Centre's Cyber Security Posture report, which praised Canada for its global leadership in cybersecurity. Nevertheless, Canada's allies expect it to take on a more prominent role in contributing to key efforts.



Accordingly, Carvin's research suggests that intelligence can be used as a powerful tool of diplomacy. Her framework includes three key elements: intelligence as the final line of communication, intelligence as a tool in diplomatic negotiations, and leveraging intelligence to achieve specific outcomes, such as using intelligence in security and defense to enhance resilience. This framework is particularly relevant in engagements with countries outside the Five Eyes network. Carvin proposes that in the future, Canada should deepen its cooperation with Japan and Taiwan to gain valuable insights into China.

Additionally, she highlights the importance of ongoing investment in intelligence liaison personnel stationed abroad to foster stronger international partnerships. As the global security landscape evolves, Carvin argues that Canada and its allies must adapt by diversifying intelligence-sharing collaborations to address emerging threats, all while preserving strategic autonomy and maintaining public trust.



Vincent Rigby highlights the escalating strategic competition with China and Russia as key drivers for expanding intelligence cooperation beyond the Five Eyes. The geopolitical challenges these two powers pose are multifaceted, involving both military and non-traditional threats, such as hybrid warfare, economic coercion, and cyberattacks.

As a result, Rigby advocates for deeper collaboration with countries in Europe, Asia, and the Indo-Pacific, where these threats are most pronounced. In an increasingly complex global security landscape, while the Five Eyes network remains crucial, it is no longer sufficient. However, before seeking new alliances outside the Five Eyes, Rigby suggests that Canada must first ensure it is fulfilling its role as a reliable ally within this established framework. When considering potential new partnerships, Canada should be strategic and selective, establishing clear criteria for engagement beyond the Five Eyes. He underscores the need for ethical standards, multilateral frameworks, and global norms in intelligence-sharing to ensure that new partnerships are effective and accountable.

For Canada, expanding intelligence cooperation presents both opportunities and challenges, offering the chance to lead in creating a more inclusive, multilateral intelligence-sharing system that can address the evolving security threats of the 21st century.



# Panel 4: The Future of Geopolitics

## **Simon Miles**

Associate Professor, Sanford School of Public Policy,  
Duke University

## **Emily Whalen**

Non-Resident Senior Associate, Center for Strategic and  
International Studies (CSIS)

## **Joseph Torigian**

Associate Professor, School of International Service,  
American University

## **Moderated by Tim Sayle**

Associate Professor of History and Director of the International  
Relations Program, University of Toronto and CASIS Vice  
President

Emerging technologies, rising authoritarianism, and new forms of conflict are challenging traditional geopolitical power structures. As the influence of major powers like China and Russia grows, the liberal international order that has governed global relations since the end of World War II is being tested. The lines between war and peace are becoming increasingly blurred, with cyberattacks, economic leverage, and disinformation campaigns taking center stage in modern statecraft without reaching the threshold of conventional military conflict.

In this dynamic environment, navigating complex alliances, adapting to evolving threats, and innovating diplomatic strategies will be critical for shaping the next era of global governance and security.






Simon Miles identifies the “Network of Autocracies” as a growing alignment among authoritarian regimes, including China and Russia, challenging the liberal international order that has dominated since World War II.

These autocratic states are collaborating to promote state-controlled economic and political models while resisting democratic ideals and suppressing dissent both domestically and internationally. This has contributed to the erosion of liberal ideas, whereby rising authoritarian regimes undermine principles such as free trade and democracy. It has also led to geopolitics shaped by hybrid forms of conflict—such as covert influence and non-violent methods of statecraft—which increasingly blurs the distinction between war and peace.

States engage in indirect "grey zone" conflict to achieve their goals, including cyberattacks, information manipulation, and digital warfare, allowing states to shape political outcomes, disrupt economies, and influence public opinion. Further, as traditional military conflict becomes too costly or politically risky, states are increasingly relying on economic leverage, sanctions, cyberattacks, and disinformation as primary tools to pursue their geopolitical interests.

Using non-military means to achieve political objectives has become the primary means by which nations exert strategic influence and achieve their political goals in a complex and interconnected world. This represents a transformation in how states assert power and pursue their interests on the world stage.





Emily Whalen discusses how the end of colonialism and the rise of new nation-states in the mid-20th century reshaped global politics, and introduced new dynamics in the 21st century. She emphasizes that while the future of geopolitics presents significant risks, it also offers opportunities for reforming global governance and fostering strategic cooperation on a range of global issues. She emphasizes the need to invest in deterrence and intellectual creativity to focus on the disruptive activities conducted by states below the threshold for conflict. This includes strengthening traditional deterrence while investing in new technologies and strategies and promoting creative thinking and cross-disciplinary collaboration to address the complex, dynamic challenges of the modern world.

Joseph Torigian highlights the growing complexity of the global order, marked by great power competition, the rise of authoritarianism, and the interplay between ideology, technology, and domestic political dynamics. Russian and Chinese leaders are using statecraft to maintain domestic legitimacy and expand their global influence. As the U.S. faces growing competition from these rising powers, Torigian emphasizes the importance of understanding the ideological motivations and technological strategies driving this shift.

For example, President Xi Jinping's ideological motivations are centred around restoring China's historical status as a great power, maintaining the primacy of the Communist Party, and reshaping the global order in ways that reflect Chinese values and interests. This involves challenging the liberal international system, expanding China's economic and technological influence, and asserting control over disputed territories. Xi's vision for China involves national rejuvenation, technological innovation, and geopolitical leadership, positioning China as a central actor in the evolving global power structure.

# Concluding Remarks

The conference underscored the critical role of intelligence in navigating a geopolitical landscape of looming and open war – for governments, intelligence agencies, the private sector, and citizens. These dynamics, changing at an ever-increasing pace, mean that all tools at our disposal – classified or not – should be leveraged, and there must always be a feedback loop to continuously adjust and improve intelligence tradecraft and technologies. In doing so, a meaningful way to maintain public trust and accountability is to maintain sound policies and governance frameworks. To best prepare for the challenges ahead, panelists reflected upon the importance of collaborating across sectors and building new alliances.



# 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), the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and the Canadian Security Intelligence Service (CSIS) for their support!

