

THE FUTURE OF CANADIAN INTELLIGENCE

**Highlights from the
CASIS Annual Symposium**

November 8, 2019

 **CASIS-ACERS**

This report is based on the views expressed during an annual symposium organised 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 does it represent any formal position of the organisations involved.

<http://www.casis-acers.ca/>

Report by Nyiri DuCharme

© 2019 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 in Canada on security and intelligence issues. A distinguished board of directors comprised of professionals of national and international reputation and status oversee the operations of the association.

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

What We Do

For over twenty-five years CASIS has held an annual meeting and has sponsored conferences, symposiums and forums on particular 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 Canadian Intelligence

Highlights from the
CASIS Annual Symposium

November 8, 2019

Table of Contents

Canadian Association for Security and Intelligence Studies.....ii

Keynote: The Future of Intelligence.....1

**Panel: Artificial Intelligence, Big Data, and Change
in the Canadian Intelligence Community.....3**

Presentation: The Future of OSINT.....5

**Panel: New Challenges for Strategic Intelligence –
Canada, United States, Private Sector7**

Closing Remarks.....9

Appendix: CASIS Symposium 2019 Program.....10

KEYNOTE

The Future of Intelligence **Dr. Shay Hershkovitz**

Technology is no longer padding our abilities to do intelligence work more effectively or efficiently, but rather, it is now structurally changing *how* we do it and *who* does it.

- Intelligence and technological advances have historically moved in tandem.
- However, with the pace of progress having become exponential, the intelligence community is now playing catch-up.
- There is an increasing role for private sector and academia in intelligence, whether or not government is welcoming them into the fold.

The future of intelligence is not about creating a new discipline. It is about radical information gathering and analysis, and the methodological changes we need to make in terms of outputs, stakeholders, roles, and safeguards. That is to say, the future of intelligence needs to consist of a revolution, not evolution, of intelligence practices.

- Despite the fact that technology has always had a key role in intelligence, traditional intelligence organizations have remained fixated on the intelligence cycle.
- We now live in an age of exponential technology. The fusion of emerging technologies, including sensors, artificial intelligence, robotics, synthetic biology, virtual reality, and 3D printing, will shape intelligence.
- Internet of Things: 50 billion devices are expected to be in circulation by 2020, jumping to 100 million by 2025. Where will we store all of this data? How will we use it?
- The flood of information will speed up the rate of Artificial Intelligence usage since machines learn faster from larger datasets.

The implications are that traditional intelligence organizations will lose their monopoly on the control of information. Off-the-shelf tools are allowing other organizations and individuals to collect and analyze more data, and it is becoming more difficult to distill this data into one actionable intelligence product.

Intelligence organizations will need to:

- Decide which data to store, for how long, to what standard, who will look at it, and how civil liberties will be protected; and,
- Work with intelligent machines while being aware of their limitations (and ours).

Is there an opportunity for new disciplines in intelligence? Temporal Intelligence (TEMPINT), similar to activity-based intelligence but with greater private sector collaboration, assumes that most individuals will be monitored as a matter of routine. Crowdsourced data (CROSINT), has particular utility in the collection and analysis of large quantities of data, and the potential to predict geopolitical events.

- As new events occur, TEMPINT analysts can look through old, private sector data to “turn back the clock” and see what happened in the lead-up.
- However, there are ethical concerns around TEMPINT, as it collects data even on those not being targeted. We collect data without knowing if we will need it.
- CROSINT does not require any element of secrecy, and it blurs the lines between collection and analysis. In some cases, the crowd will already have the data, or can be encouraged to go find it and analyze it (see: the Good Judgment Project).
- Contrasted with HUMINT and OSINT, CROSINT actively encourages participation by non-traditional intelligence partners. The new generation of crowdsourcing will bring together people and machines to collect and analyze crowdsourced data.



The future intelligence analyst will require a diversity of skills. She or he must be connected, a curator, a collaborator, creative, critical, and a content-expert.

- It is no longer possible to collate all the information in one place, there is simply too much of it. We need to create new deliverables (no one reads long reports anyways!).
- Change is taking place all around traditional intelligence organizations. Speed and relevance will determine who prevails. We need to encourage this culture of innovation, removing barriers, and decentralization of knowledge.
- Some of us are techno-optimists, and some are techno-pessimists: we need to define our appetite for the relative trade-offs including between human and artificial intelligence cognitive capabilities, maintaining transparency and judgment.



Artificial Intelligence, Big Data, and Change in the Canadian Intelligence Community

Isabelle Desmartis, Benoit Hamelin, Samuel Witherspoon, Jonathan Calof

It is becoming increasingly difficult for intelligence analysts to provide advice. We have to look at non-state actors, at insurgency groups, and at what is being done by state actors below the threshold of conflict.

- With the deluge of data, artificial intelligence becomes an attractive solution to allow analysts to focus on the “so what”, but we need to be conscious of the implications.
- Recognizing the artificial intelligence expertise in Canada, we must not reinvent the wheel. Instead, let's access this innovation. One avenue is through the Innovation for Defence Excellence and Security program at Defence Research and Development Canada.


The main challenge is that in defence intelligence, the room for maneuvering is extremely limited. “Explainability” is crucial in life-and-death scenarios.

- Machine Learning processes are only as good as their training data. It is difficult for the government to provide enough of it, since it takes effort and time to produce, ensure there is no bias, and account for privacy considerations.
- Algorithms have a short shelf-life. A package made for a particular context, like desert operations, is unlikely to work in an urban environment. We must therefore constantly improve or make new algorithms. Our procurement processes are not well-adapted.
- Across the Five Eyes partners, there is a common baseline understanding of each others' analyst training and tradecraft requirements. Analysis conducted by artificial intelligence cannot necessarily be shared in the same way. Will we need to provide caveats to indicate when a human or an algorithm has conducted the analysis?

Artificial Intelligence practitioners and experts congregate around a few start-ups. They have little connection with government; we must therefore encourage more innovation transfer. However, there are multiple obstacles:

- Intelligence agencies are not keeping pace with industry expectations;
- Data scientists from industry need to have their needs met in accessing relevant data to conduct tests and analyze for signals of interest; and,
- Classification issues persist around sharing sensitive information with partners.

These issues must be addressed in order to be able to fully revolutionize intelligence.



Lessons from private sector competitive intelligence can be useful for the public sector: to successfully execute on your strategy, you need to know your surroundings. In the era of big data, the risk of *bad* data is high. This can come from many sources, including governments with resources to overwhelm and obfuscate.

- Given this, how do we figure out how to make informed decisions? Clients are flocking to big data, which suggests an interesting role for the intelligence community in educating the client, or decision-maker, on how to interpret unreliable information. In the short-medium term, the best way to validate data remains HUMINT, especially value-added, second-level intelligence.

The prospect of big data is daunting: how much is enough, and how good is enough? Similar to TEMPINT, we do not know what we want from it yet. Countries with cheap labour can more readily collect and analyze this. To compete, Canada and its allies should build workflows and intelligent automation to assist humans in annotating the data.

- We should use artificial intelligence to filter, and make our jobs easier, especially as volumes and velocity is increasing. This will reduce the cognitive load on our human analysts, without needing to worry about displacing human judgment.
- There will be new systems that purport to summarize millions of documents; we will need to ensure they are doing what they say they are doing. We can no longer do intelligence the same way we have always done it, just with the added benefit of technology. Intelligence organizations must work with academia and the private sector to train human analysts with new skill sets.
- We also need to make decisions related to storage: what are the rules? What if we do not yet know what we should be keeping?

Is “explainability” *really* all that important? It could be argued that while we have a philosophical interest in it, it is not necessary in artificial intelligence. We already have issues around confidence in human decision-making, since we know humans are fallible.

- However, decision-makers need to know why. We can see an artificial intelligence-human compound system as a collection of experts offering different perspectives. In the analog world, a detector dog is just a sensor, not the decision-maker; the officer trained in reading its body language provides the explainability.

We often use historical data because it is what we have available, but we know humans are biased. The notion of unintended bias in artificial intelligence stems around shifts of values that have made it so that certain trends that were present historically are no longer in alignment with more modern values.

- Simply scrubbing it would mean decisions become less data-driven. Instead, discussing bias is valuable, and minimizing the impact of it in our data is important. The challenge is in acknowledging that we still fail to control for it as a society.

Monitoring the tones of foreign media and literature was historically important in signalling changes to political and military decision-making. However, this relied upon institutionally generated content, based on formal distribution of information through an established structure. With the breakthrough of the internet, the role of OSINT has changed.

- 67% of the world population uses a mobile device, and 42% are social media users. This has led to an exponential increase in the amount of user-generated content. Even in active conflict zones, internet connectivity has remained relatively stable.
- How much news is now generated by tweets? How many images are we seeing in high definition from war zones, in real-time? We are receiving *more* and *better-quality* data, including of the same event from multiple perspectives, allowing us to analyze more deeply.
- The primary change factors have been immediacy, volume, medium, and coverage. What does the “digital human terrain” look like in different places?

“

The future is already here, it's not just evenly distributed.

– William Gibson

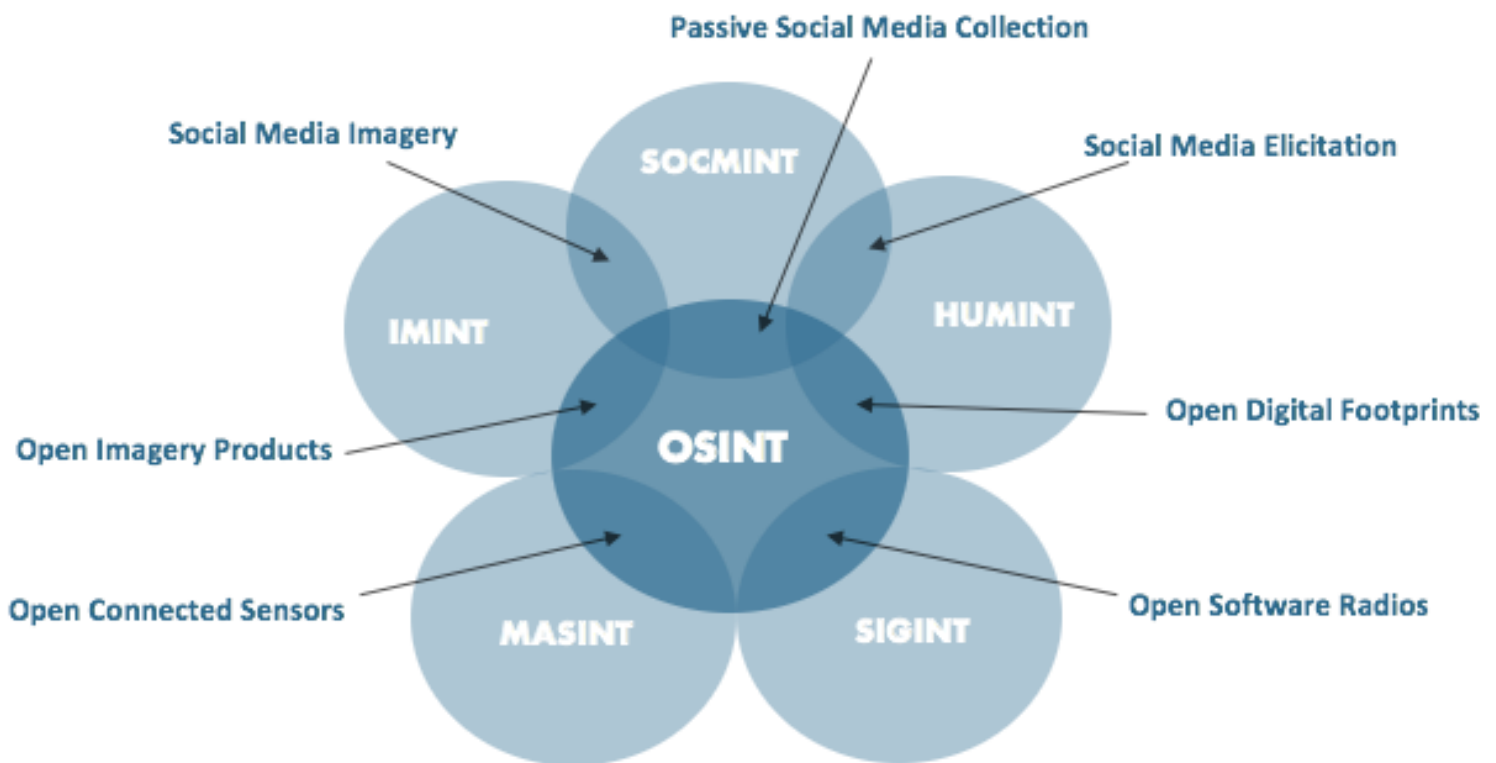
”

Big (visual) data: in 2015, 400 hours of video were uploaded to YouTube per minute, and as of 2019, Instagram has over 1 billion daily users. With this torrent of information, individuals are able to collect and geo-reference social media sightings of military equipment, and artificial neural networks can be trained to identify munitions in real-time.

- There are a number of challenges that have been introduced by these developments: the veracity of video and remaining vigilant to identify augmented data or deep-fakes; the curation of social media platforms; and, the aggregation of OSINT from multiple sources.
- Online sensor data is available, including commercial flight radars, seismological data, and spatial or hyperspectral imaging. It gets analytically interesting when mining and combining open data and imaging, including interferences, to detect patterns or abnormal behaviours.
- Service providers have realized how their platforms are being abused. The algorithmic enforcement of content, including by restricting APIs, means many tools no longer work. Fact-checkers and open researchers have lost important digital assets, and some OSINT sources are increasingly protected, as with other, more covert intel sources.

OSINT tradecraft is becoming increasingly important, particularly in the age of leaks – combining this data enables sophisticated analytics. But gray areas remain: if active acquisition approaches are needed, can we really call it OSINT? What constitutes OSINT, and what does not? What are the ethical and legal issues in using leaked materials?

MAPPING THE INTs



Ultimately, what is the nature of OSINT: is it the art of identifying the full diversity of open-source opportunities that exist, or the art of figuring out how to exploit the different open sources effectively? What is an OSINT analyst? The future of OSINT will include:

- Creativity in source development in an increasingly data-rich world, increased automation in collection and processing, dual-use potential from ISR solutions, analytic opportunities in mining and combining open data, and implications to analyst training and development.
- Working better with the private sector and academia on OSINT, including both collection and analysis, as well as red-teaming to identify gaps and blind-spots.
- Understanding that it will become increasingly difficult to act covertly, particularly when determining what open data sources to obfuscate, to saturate, or with which to interfere in order to cover your own tracks.

Intelligence organizations need to critically look at how they structure operations, how they define boundaries, and how to step up their game to exploit opportunities. This comes back to having awareness and flexibility, which does not always come naturally, as well as how we develop our OSINT capabilities.



New Challenges for Strategic Intelligence – Canada, United States, Private Sector

Jessica Davis, Thomas Juneau, Stephanie Carvin, Stephen Marrin, Kevin O'Brien

How does intelligence support policy-making, and how can intelligence products become more useful? What lessons can Canada offer other intelligence communities?

- The Canadian intelligence assessment community offers uneven service to senior policy-makers, with pockets of both excellence and mediocrity. Much of the recent improvement has been due to “electroshocks”, including the arrival of new threats which trigger changes to processes. But how sustainable is that progress?
- As a safe country, Canada's intelligence culture is less mature and sophisticated relative to that of our allies. Intelligence and national security are not the top priorities for the public service nor for politicians. Moreover, Canada is a net receiver of intelligence and often has little ability to control for information that aligns with our priorities.
- Intelligence literacy in the policy community is low, and the inverse is also true; intelligence which is too tactical often does not support whole-of-government policy-making. Information overclassification is rampant, and OSINT is still under-utilized.
- The intelligence community continues to experience recruitment and retention challenges. More exchanges and secondments would allow for cross-pollination. A new intelligence analyst classification would introduce professional standards and mandatory training.

There is little blatant politicization of intelligence in Canada, but ‘softer’ politicization – the act of making intelligence responsive to political and policy priorities – is apparent and often necessary. In recent years, Canada has developed much better coordinating institutions, including three Deputy Ministers’ committees: DMNS, DMIA, and DMOC.

- Filtering intelligence to be appropriate for public decision-making is difficult, though the trend in Canada is heading in that direction. This dilution makes intelligence more high-level, but it is nevertheless something at which we should become better. Intelligence products should better address policy priorities, and use placemats and visual aides.
- Changes in leadership have a disproportionate impact in intelligence policy-making. Other countries have more established institutional cultures, where an individual decision-maker's appetite does not have as much sway.

With new review and oversight bodies, the structure of the Canadian intelligence community keeps changing. Most senior officials support having a review mechanism, and are confident that these efforts contribute to the social license offered by Canadians that allows intelligence organizations to operate.



The US government is working hard to leverage the capacity of technology in intelligence. Data science has been identified as a key characteristic of future intelligence analysts.

- The epistemological foundation has not changed; our ways of knowing and understanding will remain at the core of human intellectual enterprise. The core function of the analyst will remain deductive, increasingly supported by technology.

The role of the private sector in intelligence analysis – both as consumer and as purveyor of solutions and services – is increasingly replacing what has traditionally been held by the government. It now has the capacity to directly participate in joint efforts.

- The provision of cyber-threat services and secure identity services contribute to threat intelligence development, offering new ways to develop HUMINT and SIGINT sources. The private sector can now support offensive tactics, including covert operations.
- The private sector can also address the issue of having bespoke, curated specialist information available to contract intelligence services at the right time. This includes language specialization, mastery of emerging technologies, and regional niche access.
- However, this opens new recruitment risk when talent exits the traditional intelligence organizations to pivot to the private sector, only to be contracted back into government.
- The private sector can also provide advanced analytic capabilities, particularly around the volume, veracity, and variety of information. Recently, i2 has been the go-to solution for passive intelligence analysis, but more modern data enrichment services use artificial intelligence and machine learning to handle massive amount of content, make sense of it, and present to humans in a way that makes sense.

Public-private partnerships are unavoidable in our knowledge domain, but private companies have different motivations than intelligence organizations. Does this present a risk? What can be done to demarcate the roles between sectors? As we introduce new review regimes, what does that mean for accountability and how we define public goods?

- Similar to the growth of private military companies in the 1990s, the intelligence realm is witnessing a rapid injection of private enterprise.
- Each individual intelligence authority in Canada has its own dialogue with the private sector as a need arises, on case-by-case bases. However, there is no management or governance of these relationships across the overarching discipline.
- How do we treat data in a way that respects Canada's legislative framework? What is a data trust? How do we interact with the people whose data this is?

Ongoing issues within the intelligence discipline include professionalization, standardization, and a sense of community. Organizations can be decentralized, but the benefit for the wider community is on exchanges across silos, including through formal and informal learning groups, and explicit professional exposure to other partners.

CLOSING REMARKS

Greg Fyffe, Dave McMahon, Ian Speigel, Holly Porteous

The promises and challenges of big data: ultimately, there is significant progress in computing power and algorithms, but also severe limitations on what solutions they can offer. This can be a frustrating time if expectations are too high.

- We need to better understand what is going on under the hood: are we accounting for bias? Are we asking the right questions to analyze our data? Is having lots of data the same as having lots of information?
- There is an ever-increasing need for people, skills, and talent to go along with this progress. What will the analyst function become? We have shifted to a situation where the flows of data from various sources is so vast that the analyst must be equipped to request, “here is the type of information I need, find me something I can use”.

These lessons are not only relevant for traditional intelligence organizations. The private sector has had consistent experiences, with various episodes (including Y2K, 5G, and quantum computing) triggering events in the private intelligence community. Partnerships across all sectors, including with academia, are key.

- The consensus is that all the converging technology, and big data, is having huge impacts.
- Artificial intelligence will be part of the solution, but is first invoking transformative changes of intelligence organizations, including reflections on how we acquire and utilize data.



There remain tensions around the centrality and importance of data collection, as well as defining our societal values on privacy, explainability, and accountability. However, we are confident that Canadians will show the same ingenuity and resilience through this transformative time that we have expressed throughout our history.

- Given our place at the forefront of developments in quantum computing and other revolutionary technologies, we must remain vigilant to the national security implications.
- We need to invest not only in good intelligence analysts, but we also need people who understand the law, and people who can translate more intelligence into policy priorities.

Appendix

CASIS Symposium 2019 Program

CASIS Symposium Program
Friday, November 8, 2019
Canadian War Museum

The Future of Canadian Intelligence

8:00	Registration Opens
8:30	Coffee
9:00	Introduction to Conference and opening speaker, Greg Fyffe, President CASIS
9:15	<i>The Future of Intelligence</i> , Dr. Shay HersHKovitz, XPRIZE Foundation
10:15	Break
10:45	<u>Panel One</u> <i>Artificial Intelligence, Big Data, and Change in the Canadian Intelligence Community</i> Chair and Discussant: Isabelle Desmartis, ADM Science and Technology, DND; Chief Executive Officer Defence Research and Development Canada Benoit Hamelin, Element AI Samuel Witherspoon, Founder and CEO of IMRSV Data Labs Inc. Jonathan Calof, Professor of International Business and Strategy, Telfer School of Management, University of Ottawa
12:00	Lunch
13:00	<u>The Future of OSINT</u> , Veli-Pekka Kivimäki, Senior Analyst, Finnish Defence Research Agency, Concepts & Doctrine Division / Strategic Analysis. Introduction: Julia Johnston, CASIS Carleton University.
2:15	Break

- 2:45 Panel Two *New Challenges for Strategic Intelligence (Canada, US, Private Sector)*
 Chair: Jessica Davis, President Insight Threat Intelligence, Former
 Senior Strategic Analyst, CSIS
 Thomas Juneau, University of Ottawa
 Stephanie Carvin, Carleton University
 Stephen Marrin, James Madison University
 Kevin O'Brien, Accenture
- 4:00 Wrap-Up Panel Greg Fyffe
 Dave McMahon, Clairvoyance
 Ian Speigel, Manager Cyber Assessments, Canadian Centre for
 Cyber Security
 Holly Porteous, Parliamentary Library
- 4:30 Close