WHO CONTROLS THE FUTURE ARCHITECTURE OF INFLUENCE?

Date: November 20, 2025

Disclaimer: This briefing note contains the encapsulation of views presented by the speaker and does not exclusively represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

On November 19, 2025, Dr. Emma L. Briant presented, *Who Controls the Future Architecture of Influence?* at the 2025 West Coast Security Conference. The session was followed by a question-and-answer period with audience members and CASIS Vancouver executives. The presentation examined the rise of influence cartels, the structural capture of digital infrastructure, the national security implications of surveillance capitalism, and the need to restore democratic oversight over the systems that shape public discourse.

NATURE OF DISCUSSION

Democracies face a systemic struggle over the extraction, ownership, and control of data, the core components of what Dr. Briant terms the "architecture of influence." The threat from disinformation is presented as structural as opposed to a discrete content problem; rooted in concentrated platform ownership, opaque algorithmic systems, and public-sector dependency on private infrastructure. Restoring democratic control requires reforms focused on data custody, algorithmic transparency, reduced monopoly power, and investment in pluralistic public-interest information systems.

BACKGROUND

Dr. Briant described a "quiet revolution" in control over the systems that determine what information societies see, prioritise, and believe. She framed the defining security challenge of the current era as control over privatised influence tools built on mass data extraction, opaque algorithmic governance, and monopolised infrastructure ownership. These systems generate a form of power capable of shaping popular perceptions, market shapes, and political outcomes beyond traditional democratic oversight.

Drawing on Sarah Lamdan's concept of "data cartels" (2023), she stated that large technology firms function as gatekeepers controlling information flows, behavioural insights, and monetisation channels. Concentrated ownership of data and advertising infrastructure allows these actors to weaponise asymmetries in access and knowledge. She noted that this concentration has geopolitical implications, particularly in the context of AI competition between the United States and China, while Europe remains comparatively disadvantaged in strategic technological capacity.

Dr. Briant stated that policy responses have largely focused on combating misinformation rather than addressing the structural business models that incentivise behavioral manipulation. Data extraction and algorithmic amplification are embedded in commercial architectures optimised for engagement and profit, not accountability. Platforms, data brokers, and cloud providers increasingly function as critical infrastructure without corresponding public obligations. Weak antitrust enforcement, deregulation, and underinvestment in civic media have enabled consolidation, while governments have outsourced communications and data management to private firms, reinforcing dependency.

Dr. Briant characterised surveillance capitalism as a national security risk. Concentrated control over digital advertising markets and information infrastructure enables influence capture, reduces plurality, and creates vulnerabilities exploitable by both domestic extremists and foreign adversaries. She cited monopoly power, declining transparency and accountability in platform governance as indicators of structural capture. Control over digital infrastructure can translate into political leverage, particularly where ownership aligns with ideological or geopolitical interests.

Dr. Briant noted that governments increasingly operate on private digital systems across military, intelligence, electoral, and policing domains. This dependency creates an "influence industrial complex," in which public institutions rely on private firms that simultaneously shape data policy through lobbying and regulatory influence. Consolidation of infrastructure under actors with extremist or authoritarian affinities can thereby increase the risk of coercive influence and strategic manipulation.

Dr. Briant described authoritarian states as exploiting democratic infrastructure vulnerabilities through investment, data brokerage, and narrative operations;

with commercial data flows providing intelligence insights comparable to traditional espionage. Absent coordinated foreign ownership reviews, transparency requirements, and research access, these vulnerabilities risk weaponisation by malicious actors.

Dr. Briant identified four structural vulnerabilities to address if we are to restore democratic control: concentration, opacity, dependency, and coercion. She recommended treating information power as critical democratic infrastructure rather than a purely commercial asset. Proposed remedies included structural separation between influence industries (advertising and algorithmic amplification) and information infrastructure (news, search, social media, AI systems), strengthened antitrust enforcement, public investment in non-profit media and open-source infrastructure, and continuity-of-consent obligations ensuring that significant changes in platform or technology company ownership or purpose trigger regulatory review and informed user consent requiring opt-in for ongoing use of data.

Dr. Briant concluded that democratic resilience depends on reclaiming three levers of influence governance: data custody, algorithmic transparency and control, and independent pluralistic information systems capable of operating without political or commercial coercion.

Question and Answer

What are the biggest challenges in maintaining a reliable, incident monitoring system within the current information landscape?

Dr. Briant emphasized the importance of research access and transparency. She noted that regulatory frameworks in Europe provide some mechanisms for data access, but coverage remains uneven globally. Researchers increasingly face defunding, legal challenges, harassment, and media campaigns, limiting independent oversight and enforcement capacity.

What new and upcoming technologies, such as generative AI, pose the biggest threat to the defence against an information war? How would we, if possible, monitor and alleviate the threat?

Dr. Briant suggested that state actors may attempt to shape model training data or outputs, while limited transparency complicates attribution and mitigation. She stressed the need for journalist education, stronger regulatory frameworks, and research access to understand and address these dynamics. Without safeguards, AI systems risk reinforcing singular or distorted narratives.

Where do you think governments are falling short in countering violent extremism? What does success look like?

Dr. Briant argued that regulatory responses remain overly reactive and containment focused. Democracies must move beyond minimal compliance strategies toward building technology ecosystems aligned with democratic values. Platforms differ in design and incentives, and regulatory frameworks must account for these distinctions. Success, she suggested, would involve structural reforms that reduce monopoly power, strengthen domestic technological capacity, and align digital infrastructure with public-interest objectives rather than profit maximization.

KEY POINTS OF DISCUSSION

- The central security challenge is structural capture of the "architecture of influence" through concentrated ownership, opaque algorithms, and data monopolization.
- Government dependency on private digital infrastructure creates national security vulnerabilities and conflicts between profit incentives and democratic accountability.
- Surveillance capitalism and influence cartels amplify risks of domestic manipulation and foreign exploitation.
- Restoring democratic resilience requires structural reform: antitrust enforcement, data custody protections, algorithmic transparency, reduced dependency on private monopolies, and investment in pluralistic public-interest infrastructure.

FURTHER READINGS

Briant, E. L., & Jones, M. O. (2025). A century of propaganda studies: from pen and sword to surveillant smartphone. Critical Studies in Media

Communication, 42(1), 64–68. *https://www.tandfonline.com/doi/pdf/10.1080/15295036.2025.2464184*

Briant, E. L., & Bakir, V. (Eds.). (2024). Routledge Handbook of the Influence Industry. London: Routledge. *https://www.routledge.com/Routledge-Handbook-of-the-Influence-Industry/Briant-Bakir/p/book/9781032188997*

Lamdan, Sarah. 2023. Data cartels: the companies that control and monopolize our information. Stanford, California: Stanford University Press.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University
Available from: https://jicw.org/