ATTRIBUTION OF INFORMATION INFLUENCE OPERATIONS

Date: November 19, 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, Björn Palmertz presented *Attribution of Information Influence Operations* at the 2025 West Coast Security Conference. The presentation was followed by a question-and-answer period with audience members and CASIS Vancouver executives. The presentation examined the strategic importance of attributing Information Influence Operations (IIO) and Foreign Information Manipulation and Interference (FIMI), the operational and analytical challenges facing attribution efforts, and a structured attribution framework and assessment model. The session concluded with a discussion of how attribution can be operationalized to support effective countermeasures.

NATURE OF DISCUSSION

The discussion focused on attribution as a foundation for countermeasures against FIMI. Mr. Palmertz emphasized that attribution is not a technical afterthought but a strategic capability that underpins deterrence, response coordination, and resilience. He introduced an interdisciplinary attribution framework and assessment matrix designed to integrate analytical best practices across domains, addressing both external challenges in the operating environment and internal analytical risks faced by attribution teams.

BACKGROUND

Attribution was presented as a prerequisite for effective countermeasures against IIO and FIMI, providing the evidentiary basis for credible domestic and allied responses. Mr. Palmertz stated that attribution aligns shared threat perceptions by moving influence operations from an ambiguous gray zone into a recognized

threat category. Domestically, this enables a shared evidence-based approach necessary for a whole-of-society response, while internationally it supports alliance cohesion and coordinated signaling. Attribution extends beyond identifying the 'who' by systematically uncovering the 'how', the adversary's Tactics, Techniques, and Procedures, and crucially, the 'why': understanding strategic intent, narrative alignment, and answering the question, 'Who benefits?' This contributes to a deeper comprehension of an operation's purpose and design. He also noted that attribution functions as a signaling mechanism, demonstrating detection capability and analytical maturity to adversaries; potentially imposing operational costs by forcing retooling. However, he cautioned that antagonistic actors also may view public exposure as an indicator of effect and hence increase efforts and resources on an information influence operation.

Mr. Palmertz stated that the external operating environment for attribution is becoming increasingly complex as adversaries adopt more sophisticated methods to evade detection. These include the use of proxies, outsourcing campaigns to third-party providers, and leveraging technology to mask identities and fragment operational footprints. These developments are occurring alongside growing data scarcity, as platforms increasingly restrict analyst access through the withdrawal of application programming interfaces and other structural limitations. They are therefore often required to operate with partial or incomplete datasets, raising uncertainty and complicating confidence assessments. Concurrently, the rise of generative AI has enabled a dramatic increase in the speed, scale, and scope of content production, enabling malign actors to iterate faster than traditional countermeasures can respond, while political and legal risks for organisations publishing attribution findings have increased. The prevalence of multi-actor campaigns has also blurred attribution boundaries, complicating efforts to disentangle coordination and amplification.

Mr. Palmertz highlighted recurring internal analytical challenges that persist across attribution efforts. These include overattribution, defined as drawing strong conclusions from weak or ambiguous signals, and linkage blindness, the failure to connect related incidents over time. Team-level challenges can arise from uneven skill profiles, where technically strong analysts may lack investigative or contextual depth, and vice versa, and these gaps can result in fragmented or incomplete assessments. Cognitive risks such as perception hacking and confirmation bias were identified as particularly acute in high-stakes environments where analysts are primed to expect interference. Ethical and

methodological risks were also noted, notably in situations where data scarcity can incentivize the expansion of investigations beyond appropriate bounds. Together, these challenges underscore the need for standardized and rigorous methodology.

Mr. Palmertz introduced the IIO Attribution Framework, designed to provide a structured and repeatable method for assessing and attributing influence operations. Building on the 2022 NATO StratCom CoE and Hybrid CoE framework, the model is grounded in the triangulation of evidence versus single-source indicators. Analysts are required to systematically collect and assess three categories of evidence—technical, behavioural, and contextual—while drawing from three data source types: open-source intelligence, proprietary data, and classified collection. This structure enables teams to identify evidentiary gaps, document reasoning, and ensure that conclusions are transparent, verifiable, and reproducible. The framework has already informed attribution methodologies of, for example, Microsoft Threat Intelligence and Recorded Future, and served as one of the foundation blocks of the European External Action Service's FIMI Exposure Matrix.

In closing, Mr. Palmertz emphasised that attribution is a foundational capability rather than a secondary objective. Given the asymmetries in data access, actor sophistication, and analytical risk, structured frameworks are essential for managing complexity and maintaining analytical integrity. Active mitigation of internal analytical errors, including deliberate skill integration and avoidance of linkage blindness, was identified as critical. He further stressed the importance of distinguishing between tactical and strategic analysis, noting that adversaries adapt to attribution efforts and that both levels must be conducted deliberately and in parallel.

Question and Answer

How has artificial intelligence been used to change influence operations are conducted and how does an actor's use of AI impact the process of attribution?

Mr. Palmertz noted that AI has significantly altered how influence operations are conducted by enabling rapid audience segmentation, high-volume content generation, and accelerated operational workflows. These developments present opportunities for malign actors to scale activity beyond previous constraints,

rendering traditional communication-based countermeasures insufficient. Holistic approaches that integrate AI into analytical workflows are required for effective response, clearly delineating where automation adds value and where sensitive judgment must remain human-led. Differences in governance structures were also highlighted, with democratic systems often constrained by legal and organisational regulation, in contrast to more centralised authoritarian models.

How would you advise professionals in youth counter radicalization to integrate your findings into effective primary preventions?

Mr. Palmertz emphasised the necessity of pre-emptive collaboration across sectors. Drawing from Swedish experiences, such as the LVU influence campaign, he noted that domestic grievances among societal groups rapidly can escalate into national vulnerabilities that offer information influence exploitation opportunities to malign foreign actors when not addressed holistically. Effective prevention can, for example, include coordination between social services, law enforcement and intelligence agencies, each contributing distinct perspectives and indicators. Preparation and relationship-building before crises emerge were identified as essential to enabling coordinated, multi-vector responses when malign information influence materializes.

KEY POINTS OF DISCUSSION

- Attribution of IIO and FIMI is a strategic capability and a prerequisite for effective countermeasures, enabling shared evidence-based understanding across domestic and allied actors.
- Analysts face significant external and internal challenges, including increasing adversary sophistication, data scarcity, AI-enabled scaling, multi-actor campaigns, and recurring analytical errors such as overattribution and linkage blindness.
- The IIO Attribution Framework provides a structured, transparent, and verifiable methodology, organizing evidence across technical, behavioural, and contextual categories and integrating open-source, proprietary, and classified data. It produces probabilistic assessments (e.g., low/medium/high confidence) to ensure conclusions reflect evidentiary strength.

FURTHER READING

Palmertz, B., Isaksson, E., & Pamment, J. (2025). *A framework for attribution of information influence operations*. Psychological Defence Research Institute. https://www.psychologicaldefence.lu.se/sites/psychologicaldefence.lu.se/files/2025-02/250131_ADACio%20D1.1_Attribution%20Framework%20Report_Final.pdf

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