**CONTEMPORARY INFORMATION STRATEGIES: COUNTERING HARMFUL NARRATIVES: THE EVOLUTION OF INFORMATION OPERATIONS: FROM AFGHANISTAN TO A MODERN, HIGH-READINESS CAPABILITY**

**Date:** November 19th, 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, Mark Shepherd, Lieutenant-Commander in the Canadian Armed Forces (CAF), presented *CAF Information Operations Evolution: From Afghanistan to Modern High-Readiness Capability* 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 evolution of CAF Information Operations (IO), doctrinal development from Afghanistan to counter-ISIS operations, and the integration of IO into contemporary multi-domain military planning.

## NATURE OF DISCUSSION

LCdr Shepherd outlined the doctrinal and operational maturation of CAF Information Operations from roots in Afghanistan to a coordinated, high-readiness capability embedded within joint and coalition frameworks. Early operational lessons demonstrated the behavioural impact of influence activities, while later campaigns against ISIS accelerated integration of cyber, electronic warfare, and psychological operations under centralized command structures. Contemporary CAF IO was described as proactive, interoperable with allies, and increasingly oriented toward dominance in the cognitive domain.

## BACKGROUND

LCdr Shepherd explained that CAF Information Operations developed organically during early deployments to Afghanistan. At that time, capabilities such as signals intelligence integration and electronic warfare coordination were nascent. Operational experience revealed the strategic utility of information operations in supporting stabilization objectives.

Operations against ISIS marked a significant doctrinal shift. The campaign revealed the centrality of cyberspace and digital dissemination to adversary strategy. LCdr Shepherd referenced efforts to disrupt ISIS propaganda distribution, including targeting online dissemination channels for publications. These efforts accelerated integration of signals intelligence, electronic warfare, web operations, and civil-military activities under more unified command arrangements within the Canadian Joint Operations Command (CJOC) and the Strategic Joint Staff (SJS).

CAF doctrine increasingly aligned with NATO standards, emphasizing interoperability and coordination across domains. The cognitive dimension of operations – how narratives shape perception, morale, and behaviour– became a central focus. Rather than reacting to adversary messaging, CAF IO evolved toward proactive approaches.

Institutionally, the establishment of the Canadian Forces Information Operations Group (CFIOG) and the Director General Information Capabilities Force Development (DGICFD) further strengthened integration of information capabilities. Modern CAF IO encompasses cyber operations, activities in the electromagnetic spectrum, and coordination across space-enabled systems. Advanced tools, including AI-assisted sentiment analysis, social media monitoring, and synthetic training environments, were described as enhancing operational readiness and adaptability.

Interoperability with NATO and Five Eyes partners was also emphasized as critical to collective deterrence. Compliance with NATO Standardization Agreements (STANAGs), participation in joint exercises, and secure communication mechanisms such as Federated Mission Networking (FMN) support multinational coordination. Information assurance protocols safeguard integrity and confidentiality, enabling seamless integration in coalition environments.

LCdr Shepherd concluded that future IO effectiveness will depend on unified command structures integrating cyber, electronic warfare, and kinetic operations.

Mastery of digital platforms and AI-enabled tools was identified as essential to counter state-sponsored disinformation and adversary influence campaigns.

**Question and Answer**

*What can policymakers do to help build a resilient information environment that can adapt to foreign influence operations, rather than just reacting to disinformation campaigns?*

Sustained personnel investment and resource allocation should form the cornerstones building resilience in complex environments. From a military perspective, readiness depends on dedicated capabilities rather than ad hoc responses. Pre-bunking approaches, such as proactively disseminating credible information before adversarial narratives take hold, are one such means of strengthening resilience.

*From a public affairs perspective, how have information operations shifted with the development of AI?*

AI tools can enhance monitoring and analysis by processing large volumes of content. However, their effectiveness depends on appropriate training and doctrinal integration.

## KEY POINTS OF DISCUSSION

- CAF Information Operations emerged from field experience in Afghanistan as an experimental capability and matured through operational experience towards supporting stabilization objectives.
- The campaign against ISIS accelerated doctrinal integration of cyber, signals intelligence, electronic warfare, psychological operations, and web operations under centralized command structures aligned with NATO standards.
- Contemporary CAF IO operates across multiple domains, emphasizing proactive narrative shaping, cognitive effects, and coalition interoperability.
- Future effectiveness depends on unified command integration, sustained resource investment, and strong interoperability within NATO and allied frameworks.

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