



Members of the Canadian Armed Forces Talon Company conduct Reconnaissance (Recce) during Exercise Wolverine Shield/Strike at Camp Adazi, Latvia, March 7, 2023.

Photo: Canadian Armed Forces Imagery Technician

Authenticity as a Weapon: The Canadian Armed Forces' Advantage in AI-Enabled Information Warfare

ALI MANOUCHEHRI AND MAJOR TYLER CURRIE

Ali Manouchehri is currently a senior advisor with the DND/CAF AI Centre. Prior to joining the DSG, he served as the Manager of Data and Analytics in ADM(RS), DND.

Major Tyler Currie is the CAF AI Integration and Acceleration Officer who works at the DND/CAF AI Centre. Tyler has spent 16 years as part of the Intelligence Branch and has served on deployed operations in Afghanistan and in the international context with Joint Forces Command (JFC) Naples. Tyler holds a master's in political studies from Queen's as well as a Master of Management in Artificial Intelligence (MMAI) from the Queen's Smith School of Business.

The Department of National Defence (DND) and the Canadian Armed Forces (CAF) operate in an information environment where the first casualty of crisis is certainty.

For example, in a North American Aerospace Defense Command (NORAD) aerospace incident, while forces track and respond to an unidentified aircraft, commanders and public affairs teams may also face a parallel hazard—AI-generated manipulated audio, video, and text, arriving at machine speed.¹

What once demanded studios, budgets, and weeks, can now be produced in minutes with widely available AI services and editing apps, and can quickly reach the public.

This operational reality points to a different kind of challenge based on trust. Generative artificial intelligence accelerates the manufacture of persuasive but false content, altering what people believe in the first moments of an incident, complicating crisis response at the most dangerous time. When trust slips, orders take longer to issue and follow, coordination slows, and the risk of serious consequences rises.

Against this backdrop, Canada faces the same pressures across multiple mission sets. We operate with allies abroad, where close coordination of messages and decisions is critical to maintaining unity of effort in coalition operations. At home, the DND/CAF supports Canadians in moments of crisis—wildfires, floods, search and rescue—often under intense scrutiny, where communication must be fast, accurate, and trusted.

In the North, vast distance, harsh weather and modest infrastructure shape how information moves and how communities experience danger. In every one of these settings, the ability to authenticate an official signal, to reassure calmly in the face of misleading claims, and to stay ahead in the information fight is essential to mission success.

The argument is straightforward. Canada, together with its allies, can effectively compete with adversaries in terms of technical sophistication and computational power and even outperform them in select emerging technologies thanks to its highly skilled and multicultural workforce and its collaborative approach to working with allies. What matters is proving that our signals are ours, verifying new information before we act on it, and addressing the public early when we encounter mis- and disinformation. By making these habits standard across policy, training, procurement, and leadership, the DND/CAF sustains its credibility and operational tempo against state actors, proxy groups, and opportunistic individuals who seek to exploit information chaos for strategic advantage.

We do not need to out-code adversaries; however, it is imperative that we be able to prove that our signals are ours, to verify new information before we act on it, and to address the public early when we encounter mis- and disinformation.

The New Conditions of Deception

Generative systems learn from large collections of text, images and audio, then produce new material that fits those patterns. They do not reason like people.² Because they are built to mimic style rather than check facts, they can produce fluent content

“Generative artificial intelligence accelerates the manufacture of persuasive but false content.”

that looks and sounds right even when it is wrong. When that output carries familiar cues such as a known voice, official phrasing or a realistic image, people are inclined to treat it as credible.

Canadian defence operations now contend with adversaries who can generate convincing imitations of official content in minutes, not weeks.³ A fabricated article, an altered image, or a cloned voice can be produced quickly and pushed across multiple platforms at a negligible cost.

For Defence practitioners, these changes introduce three reinforcing pressures:

- **Speed.** Adversaries can inject manipulated material into the information environment while events are still unfolding. A forged audio clip of an evacuation order can spread across social media before provincial authorities have even had time to draft the real message.⁴ In an operational setting, a fabricated command fragment can reach a unit before headquarters has confirmed the actual order. Speed is the adversary's advantage, because even a short hesitation can interrupt tempo and sow doubt.
- **Cost.** Generative tools are widely available, user-friendly, and inexpensive. What once demanded professional editing suites and trained operators can now be achieved with a laptop and a few dollars' worth of subscription software. This means that hostile states, proxy groups, or even lone actors can all play at scale. Defence therefore faces not only state-sponsored disinformation but also opportunistic interference from actors with little to lose.⁵
- **Precision.** Adversaries can test and refine messages in near real time, adapting to what gains traction in specific audiences. A manipulated clip that fails to resonate with one community can be quickly re-framed and re-released to another.⁶ This iterative precision allows adversaries to tailor content not just by language or region, but by exploiting the specific narratives or fears of targeted groups, including military families, diaspora communities, or allied partners.

For the DND/CAF, the consequence is an operational environment where uncertainty can be manufactured faster, cheaper, and more accurately than ever before. An order delayed, a message clouded by doubt, or an instruction competing with a convincing imitation all erode trust. Adversaries no longer need to deceive

“Adversaries no longer need to deceive everyone; they merely need to create hesitation in enough people, at enough key moments, to disrupt coordination.”

everyone; they merely need to create hesitation in enough people, at enough key moments, to disrupt coordination.

To counter this, authentication must become a routine feature of military communications, reinforced by training and leadership until it is second nature. Authentication here refers to verifying the origin and integrity of a message within the chain of command. The broader perception of authenticity—how audiences assign trust to official communications—remains critical but is distinct from technical safeguards.

When authentication is habitual, whether in confirming orders within the chain of command, embedding markers in public updates, or rehearsing verification in exercises, tempo and credibility stay with the institution rather than with those who seek to disrupt it.⁷ In this way, it is not simply a communications practice but a form of operational security—it protects speed, safeguards unity, and preserves decision advantage.

Truth Under Pressure in a Democracy

The same dynamics that complicate operational decision-making do not stop at the tactical level. They reach into the broader environment where the DND/CAF must explain decisions to Canadians, uphold accountability before Parliament, and coordinate with allies. When synthetic material blurs what is real, the consequences go well beyond a temporary disruption in the field. It corrodes public confidence in the institutions that protect Canadians.⁸ It weakens the credibility of leaders when their words and actions can be plausibly dismissed as fabrications. And it injects friction into allied cooperation, where even fleeting doubt can slow collective decisions or distort perceptions of Canada's reliability. In this sense, synthetic manipulation is not simply a battlefield nuisance but a strategic threat that targets the very foundations of trust that democratic defence requires.⁹

Generative systems complicate trust by producing convincing imitations of official material. The deeper problem is that once the public knows such forgeries exist, genuine records can also be doubted. A video that actually shows misconduct, a document that really records a breach, or an audio clip that captures an ill-judged remark can all be dismissed as fabrications. This is what scholars call the “liar's dividend—the ability of bad actors

to escape accountability by claiming that authentic evidence has been manipulated”.¹⁰

Addressing this challenge requires more than technical verification. Institutions must build resilience through consistent communication practices, transparent correction of errors, and public education about what authentic updates look like and through which channels they will appear. When the DND/CAF openly and promptly corrects errors and explains processes, it shows that credibility comes from transparency and accountability, not from projecting a false image of perfection. When it explains in advance how official communications will be marked and distributed, it equips Canadians to recognize imposters. These practices do not eliminate the liar's dividend entirely; they help reduce its impact by making authenticity a consistent expectation rather than an afterthought.

Canada's Distinct Information Environment

The challenge of generative systems is more than a technical issue. It is a question of trust that affects how we operate in contexts that are uniquely Canadian.

Defence faces these pressures in ways shaped by our geography and our institutions. As a result of Canada's geography, we have to contend with large distances, harsh weather, and limited infrastructure, especially in the North. Institutions add their own complexity, as Canada is a federation where responsibilities are shared across levels of government, where Indigenous leadership holds recognized authority, and where continental defence is conducted through binational arrangements like NORAD. These features shape how information moves, who speaks with authority, and how trust is earned.

Unlike more centralized states, Canada's layered system of governance means that no single institution controls the narrative in a crisis. A wildfire evacuation order may come from a municipality, be reinforced by a province, and receive support from the Canadian Armed Forces. In these conditions, clarity is essential because adversaries can exploit even small gaps between jurisdictions to inject doubt.

Domestic crises reveal how pressures multiply when larger populations and multiple jurisdictions are involved. Wildfires, floods, and public health emergencies require responses that cross municipal, provincial, territorial, and federal boundaries. In these moments, a false alert that looks official or a rescindment of an evacuation order can spread rapidly across social media.¹¹ Even a few minutes of hesitation can make evacuation routes more dangerous or emergency services harder to coordinate.

Domestic crises also expose the fragility of the systems Canadians rely on. Wildfires can damage cell towers, floods can cut power, and surges in demand can overwhelm local networks. For the DND/CAF, supporting civil authorities means preparing for both physical disruption and the possibility of synthetic



A Flight Engineer with 440 Transport Squadron based in Yellowknife, Northwest Territories, helps ground guide the CC-138 Twin Otter aircraft for landing at Tuktoyaktuk Airport as part of Operation NANOOK-NUNALIVUT on March 3, 2026.

Photo: Corporal Borden Webb-Brown, Imagery Technician, 14 Wing Greenwood

interference arriving at the same time. In Canada's North, conditions for communication are different and the consequences of confusion can be immediate. Towns are small, close-knit, and often distant from large centres. Infrastructure is modest, and communications can be disrupted by weather, geography, or limited bandwidth.¹²

In many communities, word-of-mouth, local radio, and community Facebook pages are still go-to communication channels.¹³ That closeness is a strength, but it also makes northern communities vulnerable. Rumours spread quickly because people care deeply for one another and act fast when they believe neighbours may be at risk. A fabricated message about a missing person, a hazardous spill, or an evacuation order can travel at the speed of conversation, long before an official update is noticed or believed.

For the DND/CAF, this means credibility in the North cannot rest only on technical fixes. It depends on human relationships that are built long before an emergency. Indigenous elders, local broadcasters, and community leaders often carry more authority in practice than distant officials.¹⁴ When the DND/CAF works with these actors to model authentic communication and demonstrates it during routine patrols, training exercises, and seasonal operations, it invests in a network of trust that is uniquely Canadian. These networks do not just pass along information, they translate it into the cultural and linguistic context of the community, making it both recognizable and actionable.¹⁵

The strength of this approach comes not just from visual cues like logos or branding—which can be copied—but from the trusted individuals who share information with established credibility and who are well-regarded. This includes trusted knowledge bearers who may have specialized knowledge and best understand how to reach the greatest number of individuals in their respective communities.

When residents know what an official message looks like and where it will appear, and when they have seen that practice tested in calmer conditions, they are more likely to disregard screenshots or forwarded messages. For the DND/CAF, this is not only a matter of communication technique, it's about respect for northern communities, recognition of Indigenous leadership, and partnership with local organizations that hold trust beyond what federal authorities can achieve on their own.

The North American and Allied Lens

In binational aerospace defence, the ability to issue trusted updates in near real time is integral. When a balloon or aircraft, for example, attracts public interest, Canadians and Americans will look for immediate reassurance.

NORAD rests on the premise that Canada and the United States respond as one, and that confidence in that unity is visible to citizens, political leaders, and adversaries alike. Timely, credible communication is therefore not an accessory to continental defence, it is one of its systems.¹⁶ Just as radar networks provide a shared view of the skies, consistent and authoritative updates provide a shared view of events.

The same logic applies to Canada's broader alliances. Coalition exercises and deployments are particularly vulnerable because they demand high levels of trust and synchronization among diverse partners. Adversaries understand this.¹⁷ A single synthetic provocation, a forged after-action report suggesting a capability failure, a fabricated image implying misconduct, or a falsified message hinting at disunity among commanders, can be timed to coincide with a critical decision point. Even if debunked within hours, such incidents consume valuable bandwidth, delay coordination, and erode confidence within the coalition.

These disruptions rarely break alliances outright, but their cumulative effect narrows the margin for error and makes collective action harder. Differences in national priorities are natural within coalitions, but synthetic manipulation weaponizes those differences, magnifying suspicion and slowing unity of effort.¹⁸

When Canada and the United States employ recognizable methods of authentication—consistent visual markers on updates, cryptographic signatures embedded in imagery and video, and habitual use of official channels—the public learns what to look for and journalists can report with greater confidence under pressure.¹⁹ In this way, authentication becomes not only a safeguard against confusion but a strategic asset that underpins the credibility of continental defence.

For Canada, credibility in allied operations depends not only on the professional conduct of our forces but also on the speed and clarity with which that conduct is represented to partners and the public alike. Authentication in this sense becomes operational currency; it buys tempo, steadies confidence, and denies adversaries the space to turn doubt into delay. Whether in continental defence, northern communities, or international operations,

the CAF requires habits of disciplined communication that are routine long before a crisis begins.

Public Affairs and the Canadian Voice of Credibility

The habits of verification that protect the chain of command must also extend to how the DND/CAF speaks to the public. Culture is expressed in the tone, timing, and clarity of how we communicate. Public Affairs therefore begins well before a crisis. If the DND/CAF explains in plain language that convincing fakes are now part of the information environment, demonstrates how authentic updates will appear, and makes a habit of steady communication when the stakes are low, the public learns what to expect when the stakes are high.²⁰ In a crisis, Canadians respond best to clarity about process: what steps are being taken to verify, when the next update will arrive, and how to avoid spreading harm while the facts are gathered.²¹

Canada's public voice must also reflect who we are. Canadians value fairness and straightforward speech. A short video from a commanding officer, posted quickly on an official channel, carries moral weight because it is both personal and institutional. A statement that sets out what information will be released and when earns credibility, because it commits the DND/CAF to a clear timeline and shows the public what to expect. In bilingual communications, speaking with equal clarity in both official languages signals care and strengthens trust. Where Indigenous communities are involved, direct engagement with community leadership in culturally appropriate ways, and through trusted intermediaries, reinforces legitimacy and helps verification habits spread.

Verification in the Chain of Command

Synthetic interference does not need to deceive an entire formation to have effect. When many elements must move together, hesitation by a single unit is enough to erode momentum, introduce risk, and give an adversary room to manoeuvre. The danger lies not in mass deception, but in the small fractures of confidence that can ripple through a formation when information cannot immediately be trusted.

This risk is not new. Armed forces have always needed ways to ensure that orders are genuine. Historically, units relied on call-signs, code phrases, or even physical couriers to verify instructions. During the Second World War, for example, challenge-and-response codes were a routine safeguard, and even in modern operations radio checks remain a basic discipline.²² The principle has always been the same; no matter how urgent the moment, units must be sure that what they are acting on is authentic. Modern communications have increased speed, but they have also multiplied the points where a false or manipulated message could enter the system. What changes in the age

of synthetic content is how convincing a forged instruction can appear, and how little time there may be to question it.²³

An unexpected order received during a manoeuvre illustrates the problem. The message may look or sound authentic, but if its timing raises doubts and there is no agreed way to check, the safest choice is often to pause until higher authority can confirm.²⁴ If the order was genuine, that pause has already cost time in a critical window. If it was false, the unit may have avoided a mistake—but only by slowing down and surrendering their initiative. Either way, uncertainty extracts a price. In a high-tempo environment, even seconds of hesitation can alter the outcome of an engagement, shift the balance of initiative, or create openings for an adversary to exploit.

Defence practice must therefore emphasize simple, rapid methods of confirmation. A pre-arranged signal, a short exchange over an alternate channel, or another agreed procedure can resolve doubt in seconds. These safeguards are not new—radio checks, challenge-and-response protocols, and confirmation through alternate channels have long been standard practice. What has changed is the operational context: synthetic audio that mimics a commander's voice with high fidelity, fabricated video that appears to show orders being issued, or text messages that replicate the style and format of legitimate communications with precision.

Current DND/CAF procedures assume that most communications can be trusted unless there is specific reason for doubt. In an environment where convincing forgeries can be produced at scale and speed, this assumption no longer holds. The gap is not that verification procedures do not exist, but that they are not consistently applied when information arrives through familiar channels. Training often focuses on verifying orders that are obviously suspicious—those that arrive through unusual means or contradict known plans—but does not routinely rehearse verification of plausible-seeming instructions that may have been subtly manipulated.

Moreover, operational constraints can limit the effectiveness of existing procedures. During domestic emergencies such as floods or wildfires, infrastructure disruption may degrade alternate communication channels, making it harder to confirm orders through independent means. Similarly, generative-AI-enabled manipulation may spread misinformation that undermines CAF operations, such as fake alerts about disasters, slowing response efforts.²⁵ In coalition operations, differences in national procedures or language barriers can slow verification when speed is most needed. And in high-tempo combat scenarios, the pressure to act quickly can override the instinct to verify, especially when an order appears to come from a trusted source.

What is required is not the invention of new procedures but the consistent integration of existing ones into routine practice, adapted to account for synthetic threats. This means rehearsing verification drills not only for obviously suspicious orders but for routine-seeming instructions that arrive during exercises. It means

ensuring that alternate communication channels are tested and maintained as rigorously as primary ones. And it means training personnel to recognize that in the current environment, verification is not a sign of hesitation but of professionalism—a discipline as fundamental as weapons handling or navigation.

Leadership is central to this discipline. Commanders set the expectation that surprising instructions are always checked, and that verification under pressure is not a sign of weakness but of professionalism.²⁶ Units that rehearse these drills in exercises will find them instinctive in operations. When leaders consistently reinforce that verification is expected, and when they acknowledge it as sound judgement rather than hesitation, the culture of an entire formation begins to shift. The result is not only to prevent mistakes, but to preserve confidence inside the chain of command when adversaries attempt to sow confusion.

Embedding Trust in Policy, Training, and Leadership

Credibility cannot rely on technology alone. It must be reinforced through the full machinery of Defence in policy, in training, and in leadership practice. Law and policy need not chase every technical novelty to be useful. They need to give clarity and confidence to those responsible for speaking and deciding. For the DND/CAF, this means that doctrine, guidance, and standard operating procedures must all reflect the reality that synthetic content is not an anomaly but a persistent feature of the environment. Policy alone is not sufficient. Training is where principles become second nature. Just as soldiers learn to conduct radio checks or execute standard drills, DND/CAF personnel can learn to handle ambiguous information without hesitation. A watch officer who encounters a suspicious clip should know immediately whom to call and what to say. A commander who receives an unusual order should be prepared to seek confirmation through an alternate channel.

The challenge is not that this knowledge is absent, but that it is not routinely practiced under realistic conditions. Current training often treats information verification as a secondary concern, addressed in classroom settings rather than integrated into field exercises. Personnel may know in principle whom to contact when they encounter suspicious material, but without regular rehearsal under stress, that knowledge does not translate into instinctive action. After-action reports from recent exercises have noted instances where units hesitated or acted on unverified information because verification procedures, though known, were not habitual.²⁷

These moments should not be left to improvisation in the field. They need to be woven into exercises at every level, from basic training to large-scale joint exercises, so that CAF members instinctively practice verification in the same way they already practice battle drills, navigation, or radio discipline.

Public Affairs officers should have language pre-cleared that allows them to act quickly when false or misleading material is



An Observer, Controller, Trainer (OCT) responsible for the evaluation of ex GLOBAL RESOLVE, tracks and updates troop movements in the training area with a Tactical Assault Kit (TAK) tablet, allowing real-time communication between different OCT elements in the field. Image taken in the Yukon Training Area near Fairbanks, Alaska, on February 17, 2026.

Photo: Cpl Dustin LeVasseur Pearce

circulating. This means they are not waiting for legal or policy approval in the middle of a crisis, but can immediately acknowledge that contested material exists, caution the public that it has not been verified, and point directly to trusted official sources where updates will appear. Having this language prepared in advance prevents silence from being mistaken for confirmation, and ensures that the first word from the DND/CAF is one of clarity and direction. Moves like these may seem minor on their own, but together they create a posture of readiness that allows operations and communications to continue steadily even when adversaries try to inject confusion. Exercises that test these communications drills, complete with simulated forgeries and fabricated clips, would make verification as routine for Public Affairs as weapons handling is for infantry.

Leadership is the hinge that turns principles into habits. When senior officers and officials model disciplined verification under pressure, subordinates see it not as hesitation but as professionalism. A commander who insists on a quick confirmation before acting on an unusual order sets a tone that spreads through the formation. A Public Affairs leader who corrects an earlier statement with the same speed and visibility as the first release shows that credibility is built on candour. These examples travel quickly inside a military culture where tone and timing at the top shape behaviour across the ranks.

Ultimately, trust must be embedded across all levels of Defence—written into doctrine, reinforced through routine training, and modelled by leaders in both calm and crisis. These three pillars—policy, training, and leadership—work together to ensure that the CAF does not face synthetic interference as an improvised challenge but as an environment for which it is fully prepared.

Measuring a Canadian Standard of Success

Defence is experienced at measuring readiness, and the same discipline applies in the information environment.²⁸ The most important measure is time. The institution must track how long it takes to classify suspicious material, provide internal guidance on confidence, and issue a trusted public update. It must also record how quickly units confirm or dismiss unusual orders through established procedures, and how often these drills are rehearsed in exercises. Just as operational readiness reports measure ammunition stocks, equipment serviceability, or personnel strength, the DND/CAF can measure information readiness by how quickly and reliably the system can validate or reject contested material.²⁹

Performance must show steady improvement, just as in other areas of readiness.

For example, if a formation currently requires twenty minutes to escalate and resolve a suspicious order, exercises should aim to reduce that to ten minutes, then five, without sacrificing accuracy or safety. If Public Affairs teams need an hour to coordinate a first statement during a domestic emergency, the goal should be to bring that down to minutes through pre-cleared language, distributed authorities, and clear escalation channels. Each iteration becomes an opportunity to shorten the cycle while strengthening trust.

Surveys and feedback loops can add further texture. Canadians should be asked whether they know where to find authentic DND/CAF updates and whether they can describe what those updates look like. Journalists and civil society partners can be consulted on whether verification tools are accessible and reliable. Allies can be surveyed on whether Canadian methods are interoperable with theirs, and whether our signals can be trusted instantly in multinational settings. These forms of measurement, though qualitative, are as critical to resilience as quantitative metrics. Scholars researching institutional trust and trustworthiness have created useful frameworks for assessing these dimensions.³⁰

They will continue to appear, and adversaries will continue to innovate. Success will mean that Canada responds calmly, speaks quickly, and retains trust when they appear. In practice, this

translates to fewer pauses in operations because of unauthenticated instructions, fewer instances where false alerts outpace real ones during domestic emergencies, and fewer occasions where fabricated narratives distract from the purpose of allied exercises or deployments. When measured consistently, these benchmarks allow Defence to know not only whether it is prepared, but whether Canadians and allies share confidence in that preparation.

Conclusion

Generative artificial intelligence has transformed the conditions under which truth must compete for attention; it has made falsehood cheap, fast, and convincing. That reality touches the heart of military effectiveness.³¹ If a forged message can slow a decision, if a fabricated video can fracture allied unity, or if a false alert can pull Canadians into danger, then adversaries have succeeded without firing a shot. This is the contest in which the Canadian Armed Forces now operate.

Canada is not powerless in this fight. Defence does not need to eliminate every forgery; it needs to prove what is real faster than falsehoods can spread. That means commanders who expect verification before manoeuvre, Public Affairs teams who speak early with candour, policies and tools that make authentication ordinary, and leaders who practice discipline in communication as rigorously as they do in operations. It means making the DND/CAF voice recognizable across every setting—whether in NORAD's command posts, in northern communities, during domestic crises, or on coalition operations abroad.

The DND/CAF has always defined itself by professionalism, integrity, and the ability to act under pressure.³² In the information battles now unfolding, those same qualities are the foundation of advantage. By proving authenticity, protecting tempo, and speaking with a voice that reflects Canadian values of honesty and respect, the DND/CAF needs to shield itself from deception and protect the democracy it serves.

Notes

- 1 Joseph Vossler, Gerald Mazur, Andre Slonopas, Danyl Miller, Edward Olbrych, Aaron Sweeney, and Jacob Strahan, "Artificial Intelligence as a Force Multiplier in U.S. Military Information Campaigns," *Cybersecurity and Information Systems Information Analysis Center (CSIAIC)*, October 28, 2024. Originally found at: <https://csiac.dtic.mil/articles/artificial-intelligence-as-a-force-multiplier-in-u-s-military-information-campaigns/>.
- 2 Cole Stryker and Mark Scapicchio, "What Is Generative AI?," *IBM Think*, March 22, 2024. Originally found at: <https://www.ibm.com/think/topics/generative-ai>.
- 3 Canadian Security Intelligence Service, "Implications of Deepfake Technologies on National Security," Government of Canada, July 14, 2025. Originally found at: <https://www.canada.ca/en/security-intelligence-service/corporate/publications/the-evolution-of-disinformation-a-deepfake-future/implications-of-deepfake-technologies-on-national-security.html>.
- 4 Akshay Kulkarni, "BC Wildfire Service Faces Challenges from AI-Generated Misinformation," *CBC News*, August 6, 2025. Originally found at: <https://www.cbc.ca/news/canada/british-columbia/bc-wildfire-service-ai-misinformation-1.7602041>.
- 5 Canadian Centre for Cyber Security, "National Cyber Threat Assessment 2025-2026," Government of Canada, October 30th, 2024. Originally found at: <https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf>.
- 6 "An existential threat: Disinformation 'single biggest risk' to Canadian Democracy," *Digital Forensic Research Lab (DFRLab)*, March 19, 2024. Originally found at: <https://dfriab.org/2025/03/19/canada-disinfo-existential-threat/>.
- 7 National Security Agency, Federal Bureau of Investigation, and Cybersecurity and Infrastructure Security Agency, *Contextualizing Deepfake Threats to Organizations*, September 12, 2023. Originally found at: <https://media.defense.gov/2023/Sep/12/2003298925/-1/0/CSI-DEEPPFAKE-THREATS.PDF>.
- 8 *Increasing Threats of Deepfake Identities*, Department of Homeland Security, accessed September 29, 2025. Originally found at: https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.
- 9 Di Cooke, Abigail Edwards, Alexis Day, Devi Nair, Sophia Barkoff, and Katie Kelly, *Crossing the Deepfake Rubicon: The Maturing Synthetic Media Threat Landscape*, Center for Strategic and International Studies, November 1, 2024. Originally found at: <https://www.csis.org/analysis/crossing-deepfake-rubicon>.
- 10 Bobby Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107, no. 6, December 2019. Originally found at: <https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security>. Also see Vaccari, Cristian & Andrew Chadwick (2020). "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News." *Social Media + Society*, 6(1).
- 11 Akshay Kulkarni, "AI-Generated Media and Misinformation of N.W.T. Wildfires Circulating, Fire Officials Warn," *CBC News*, August 6, 2025. Originally found at: <https://www.cbc.ca/news/canada/north/ai-generated-media-and-misinformation-of-n-w-t-wildfires-circulating-fire-officials-warn-1.7623579>.
- 12 Alexander Dalziel and Daniel Nikoula, *Polarized: Climate Change, Geopolitics and Disinformation in the Arctic*, Information Integrity Lab, University of Ottawa, July 2025. Originally found at: <https://infoilab.uottawa.ca/com-mon/Uploaded%20files/PDI%20files/Polarized-EN-FINAL.pdf>.
- 13 Rob McMahon, Michael B. McNally, Eric Nitschke, Kyle Napier, María Alvarez Malvido, and Murat Akçayir, "Codesigning Community Networking Literacies with Rural/Remote Northern Indigenous Communities in Northwest Territories, Canada," *Journal of Computer-Mediated Communication* 29, no. 1, January 2024. Originally found at: <https://doi.org/10.1093/jcmc/zmad042>.
- 14 Department of National Defence, "Department of National Defence Indigenous Reconciliation Program - Grants and contributions," Government of Canada, March 27, 2025. Originally found at: <https://www.canada.ca/en/departement-national-defence/program/indigenous-reconciliation-funding.html>.
- 15 Jayde Lavoie, Jill Barclay, and Wilfrid Greaves, *Improving the Canadian Armed Forces' Recruitment and Retention of Indigenous People: Best Practices from the New Zealand Defence Force, North American and Arctic Defence and Security Network*, Queen's University, September 8, 2020. Originally found at: https://www.naadsn.ca/wp-content/uploads/2020/09/20-September_Policy-Brief-CAF-1.pdf.
- 16 Department of National Defence, "Joint Statement on Norad Modernization," Government of Canada, August 14, 2021. Originally found at: <https://www.canada.ca/en/departement-national-defence/news/2021/08/joint-statement-on-norad-modernization.html>.
- 17 Jill Goldenziel and Daniel Grant, "Information Resilience: Countering Disinformation and Its Threat to the U.S. Alliance System," *War on the Rocks*, November 15, 2023. Originally found at: <https://warontherocks.com/2023/11/information-resilience-countering-disinformation-and-its-threat-to-the-u-s-alliance-system/>.
- 18 Patrick Samaha, "Weaponized AI, The New Frontline in Global Disinformation Warfare," *NATO Association of Canada*, June 24, 2025. Originally found at: <https://natoassociation.ca/weaponized-ai-the-new-frontline-in-global-disinformation-warfare/>.
- 19 For current standards and ongoing initiatives, see Content Authenticity Initiative (CAI), which develops technical standards for content provenance (contentauthenticity.org), and the Coalition for Content Provenance and Authenticity (C2PA), which provides specifications for embedding cryptographic metadata in digital media (c2pa.org). NATO's Strategic Communications Centre of Excellence has also published guidance on countering disinformation in military contexts (stratcomcoe.org).
- 20 Department of National Defence, *Canadian Army Communication Strategy 2024-2026*, Government of Canada, July 15, 2025. Originally found at: <https://www.canada.ca/en/army/services/for-the-soldier/canadian-army-communication-strategy-2024-2026.html>.
- 21 Eric J.G. Storm, *Needing Unified Direction: Developing Capabilities for Operations in the Information Environment*, Canadian Forces College, 2025. Originally found at: <https://www.cfc.forces.gc.ca/259/290/950/305/StormSF50DL.pdf>.
- 22 George I. Back and George Raynor Thompson, "Military Communication," *Encyclopaedia Britannica*, accessed on September 29, 2025. Originally found at: <https://www.britannica.com/technology/military-communication>.
- 23 Di Cooke, Abigail Edwards, Alexis Day, Devi Nair, Sophia Barkoff, and Katie Kelly, *Crossing the Deepfake Rubicon: The Maturing Synthetic Media Threat Landscape*, Center for Strategic and International Studies, November 1, 2024. Originally found at: <https://www.csis.org/analysis/crossing-deepfake-rubicon>.
- 24 Daniel L. Byman, Chongyang Gao, Chris Meserole, and V. S. Subrahmanian, *Deepfakes and International Conflict*, Brookings Institution, January 2023. Originally found at: https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf.
- 25 Recent incidents show how Generative AI amplifies misinformation risks: during the 2025 Northwest Territories and British Columbia wildfires, AI-generated images exaggerated fire damage and spread widely on social media. See: *N.W.T. fire officials warn of AI-generated images, misinformation circulating online* | *CBC News*; *AI-generated wildfire images spreading misinformation in B.C., fire officials warn* | *CBC News*, and *AI-generated images exaggerated fire damage and spread widely on social media*. In 2022, a deepfake video of President Zelenskyy urging Ukrainian troops to surrender circulated online, aiming to erode morale during active combat. See: *A deepfake video showing Volodymyr Zelenskyy surrendering worries experts* : *NPR*.
- 26 Gen. Gary Brito, "Professionalism Is the Foundation of the Army and We Will Strengthen It," *War on the Rocks*, March 18, 2024. Originally found at: <https://warontherocks.com/2024/03/professionalism-is-the-foundation-of-the-army-and-we-will-strengthen-it/>.
- 27 While specific after-action reports remain classified, this observation is consistent with findings from NATO exercises on countering hybrid threats, where information verification was identified as an area requiring greater emphasis in training. See: *NATO Strategic Communications Centre of Excellence, Hybrid Threats: A Strategic Communications Perspective*, 2019.
- 28 *The Canadian Armed Forces Ethos: Trusted to Serve*, Department of National Defence, July 19, 2023. Originally found at: <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/CAF%20Ethos%20Trusted%20to%20Serve%20-%20English%20-%20FINAL.pdf>.
- 29 Department of National Defence, "CDS/DM Directive for CAF Force Posture and Readiness (FP&R) 2024/2025," Government of Canada, March 12, 2025. Originally found at: <https://www.canada.ca/en/departement-national-defence/corporate/policies-standards/dm-cds-directives/cds-dm-directive-caf-force-posture-readiness.html>.
- 30 Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709-734; and Grimmelikhuijsen, S., & Knies, E., 2017. Validating a scale for citizen trust in government organizations. *International Review of Administrative Sciences*, 83(3), 583-601.
- 31 Austin Coombs, "Persuade, Change, and Influence with AI: Leveraging Artificial Intelligence in the Information Environment," *Modern War Institute*, October 25, 2024. Originally found at: <https://mwi.westpoint.edu/persuade-change-and-influence-with-ai-leveraging-artificial-intelligence-in-the-information-environment/>.
- 32 *The Canadian Armed Forces Ethos: Trusted to Serve*, Department of National Defence, July 19, 2023. Originally found at: <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/CAF%20Ethos%20Trusted%20to%20Serve%20-%20English%20-%20FINAL.pdf>.