



A member of HMCS MARGARET BROOKE takes a photo of Christ the Redeemer as the ship transits into Rio de Janeiro, Brazil during Operation PROJECTION 25-01 on February 1, 2025.

Photo: Corporal Connor Bennett, Canadian Armed Forces Photo

Note from the Guest Editor

MATTHEW KELLETT

Dr. Matthew Kellett is Special Advisor, Canadian Armed Forces Cyber Command and Associate Editor for Cyber for the Canadian Military Journal. He started his career as a commercial software programmer. He worked as scientific support and then as a defence scientist for 15 years with Defence Research and Development Canada, researching cyber security. Since 2017, he has advised the CAF's operational cyber commanders on the operationalization of the cyber domain with a focus in recent years on concepts, doctrine, and terminology. He has bachelor's degrees in computer science and English literature and a doctorate in theoretical computer science, all from the University of Ottawa.

Welcome to this special issue of the *Canadian Military Journal* dedicated to cyber and artificial intelligence. Cyberspace is everywhere in our lives. From doomscrolling on our phones to endless emails at work, it seems like the most familiar thing in the world. At the same time, we hear about companies being compromised and critical infrastructure being attacked. It can be hard to understand how these two worlds relate.

The truth is that the part of cyberspace we interact with—the interfaces of our iPhones and Windows computers—is a thin skin over a vast infrastructure, and that thin skin makes it seem like everything works transparently as if by magic. There is no magic. There is just a complex system of systems that requires a deep technical skillset to understand.

NATO, Canada, and many of our allies recognize cyberspace as a domain of warfare. In practice, this designation is a recognition that failure to field a specialized military capability in the cyber domain risks losing our ability to operate in all the other domains: sea, land, air, and space. It is for this reason that the Canadian Armed Forces Cyber Command (CAFCYBERCOM) was

stood up on 26 September 2024 as a two-star command under Major-General Dave Yarker and reporting directly to the Chief of the Defence Staff.

CAFCYBERCOM has the Canadian Armed Forces mandate to conduct cyber operations, signals intelligence, and joint electronic warfare. These areas share similar skillsets and, in some cases, are mutually reinforcing. These capabilities are not new. They existed and were operationally effective before the command stood up. The creation of the command simplified the military reporting structure and made these capabilities easier to integrate into military operations.

In this special issue, we look at cyberspace from a few different perspectives. We start with where Canada fits into the world with our expectations about how nation-states should act in cyberspace. *Commentary: Canada as a Responsible Technology Power in the 21st Century* by Christina Marcotte examines the Government of Canada's actions in this space, including how we adapt to new technologies like artificial intelligence and how we govern our actions and link that governance to the rules-based international system.

As I noted above, most people think about phones and computers when they think about cyberspace, what we would collectively call information technology (IT), but cyberspace can be far more than that. In our *Introduction to Government of Canada*

Cyber Basics: A Primer by Alexandra Green and Dr. Matthew Kellett (me), we try to draw a more complete picture of cyberspace in simple terms. Among other things, we talk about areas of cyberspace that users rarely think about, such as industrial control systems, military platforms, and smart lightbulbs; we discuss the difference between cyber security and cyber defence; and we discuss the reason why you rarely hear the term cyber attack in official contexts.

Finally, for the cyber part of this issue, I really wanted to expose this audience to the significance of signals intelligence to military cyber operations. *Commentary: The SIGINT-Cyber Nexus in the Canadian Armed Forces* by Lieutenant-Colonel Leslie Rediger does just that. It shows how these two disciplines, while distinct, share similar characteristics and are mutually reinforcing, which is why they have been grouped together within CAFCYBERCOM.

Artificial intelligence (AI) has been a promise and buzzword for decades. Recent advancements in generative AI, starting with ChatGPT's release in 2022, have changed that conversation. While many technological trends, like 5G, have been touted as the next industrial revolution only to deliver seemingly moderate, incremental improvements, AI has all the appearances and momentum of being revolutionary. Whether you are an AI skeptic or an AI advocate, and I, for the most part, have fallen on the skeptical side of that divide, there is no denying that AI is a collection of



Participants of a Counter-Uncrewed Aircraft Systems course tour a SA-8 air defence vehicle, in Poland, on December 11, 2024.

Photo: Canadian Armed Forces Imagery Technician

emerging technologies that cannot be ignored. We must grapple with it and its implications, and failing to do so may leave us, as a nation-state, at a severe technological disadvantage.

DND/CAF recognized this threat and in May 2024 issued the DND/CAF AI Strategy. The strategy is important in that it applies equally to both DND and the CAF and must satisfy both departmental/corporate requirements and military/operational requirements, which is not an easy task. The strategy has a strong emphasis on the responsible use of AI.

One of the major pieces of the strategy was the establishment of the Defence AI Centre. In *Commentary: Forging the Future: An Integrated Canadian Defence AI Ecosystem* by Lydia Korczynska, we get a first-hand view of the strategy and its implementation in the department from the director of the Defence AI Centre. The strategy sets an ambitious target of DND/CAF being AI-enabled by 2030, and the Defence AI Centre is charged with enabling that goal.

The next two articles come from the Defence AI Centre. *Artificial Intelligence and the Sino-American Techno-Competition: Implications for Canadian and Allied Defence* by Jennifer Gearey and Major Tyler Currie uses the lens of technological competition between China and the United States to discuss how AI is reshaping the defence landscape. It outlines the need for Canada to take decisive action in four key areas: data, compute, institutions, and talent.

Allied Interoperability Under Pressure: AI, Procurement, and the Future of Defence Cohesion by Samuel Paquette and Major Tyler Currie looks at interoperability with our allies, especially NATO, and the challenges that we face. It looks at critical barriers: volatile supply chains, slow procurement systems, and diverging governance models.

The next article, *Navigation by Sextant & Astrocompass: A CAF Approach for AI Adoption* by Colonel Adam Moore and Dr. Matthew da Mota, is notable because it does not come from the Defence AI Centre, but independently raises many of the same concerns. It looks at AI's ability to disrupt military decision-making processes and what that means for how AI is implemented and used in a military context. Simply put, a commander cannot simply blame the AI if something goes terribly wrong, and that reality means that AI will necessarily be used differently in defence than in other areas.

The final article comes again from the Defence AI Centre. *Authenticity as a Weapon: The Canadian Armed Forces' Advantage in AI-Enabled Information Warfare* by Ali Manouchehri and Major Tyler Currie looks specifically at AI-enabled disinformation, which is probably the current most publicly well-known and difficult-to-solve problem from the malicious use of AI. The article offers approaches to countering such disinformation. Interestingly, the solutions are not solely technological.

“ People are a force multiplier in the cyber domain in a way that is unheard of in other domains.”

If I can leave you with one last thought before you dive into the commentaries and articles in this special issue, it is this: in this domain, people are much more important than technology. People are a force multiplier in the cyber domain in a way that is unheard of in other domains. A trained operator or specialist can be magnitudes more effective than someone who has simply been trained to use a tool. While technology can make their work easier or allow them to do more advanced things, technology alone is not sufficient to operate effectively in the cyber domain. AI may change the pace and type of problems presented by the domain, but it is unlikely to supplant people as the major force in the domain for purely practical reasons: the things we care most about in the domain, like a nation-state adversary compromising a computer network, are vanishingly rare compared to the totality of the data available. It is our people's domain expertise and honed intuition that give us the edge. AI may eventually change that equation, but it is unlikely to be soon.

I want to thank all the authors and peer reviewers for making this special issue possible. I am indebted to the Defence AI Centre for their support and significant contributions to this special issue. I am indebted to CAFCYBERCOM for their support of my role as guest editor. I want to thank the members of the command who worked on commentaries and articles for this special issue that ultimately did not make it, mostly due to conflicting operational demands. I hope to bring you some of those pieces in future issues of this journal. A big thank you to the staff at CMJ for managing this issue so professionally. Finally, I want to thank Alexandra Green who expertly guided me through every step of the editing process.

Manuscripts solicited for this issue were written in 2025 and final versions were submitted in March 2026. The necessarily long lead time between writing, final submission, and publication may impact the currency and relevancy of the information presented, especially for quickly evolving topics like artificial intelligence.