



Attorney Odessa Rossil Magisa, Officer-in-Charge of the Office for DND Information Security, listens to Major-General Dave Yarker, Commander of Canadian Armed Forces Cyber Command (CAFCYBERCOM), during a bilateral Working Group with counterparts from the Armed Forces of the Philippines Cyber Command, held on 10 July 2025 at Camp Aguinaldo, Philippines. The meeting provided an opportunity to exchange operational insights and explore cyber defence cooperation, further advancing Canada's Indo-Pacific Strategy.

Photo: Maj Christopher Daniel, CAFCYBERCOM

Foreword

MAJOR-GENERAL DAVE YARKER

In 2024 Major General (MGen) Dave Yarker was appointed as the first Commander of the newly formed Canadian Armed Forces Cyber Command. Prior to this appointment he filled multiple roles in the Canadian Armed Forces cyber community, including command at unit and formation level and liaison positions with both United States Cyber Command and Canada's Communications Security Establishment. His earlier career included employment within the tactical signals community and joint communications roles. He holds undergraduate degrees in Engineering Physics and History, along with master's degrees in Engineering Physics, Defence Studies, and Public Administration.

It is an honour and a pleasure to be given the opportunity to provide a foreword to this important special issue of the Canadian Military Journal dedicated to cyber and artificial intelligence concerns. With the recent stand-up of the Canadian Armed Forces Cyber Command and the establishment of a formal Defence AI Centre, our warfighting institution has taken some significant steps towards recognizing the importance of these two areas.

Both artificial intelligence and cyber operations are grounded in modern technology and its pervasive impact on warfighting. That impact is simultaneously deep and broad. We have placed modern technology at the heart of our way of war, driving precision in intent, location, and time in the application of violence. However, these technologies are fundamentally vulnerable, opening new avenues of attack and therefore defence, which leads to

“ The question is no longer whether AI and cyber operations will impact the western way of war, but whether we will react to the ways they already have.”

the characterization of cyberspace as a domain of warfare. For its part, AI introduces a radically different scale and speed to many technologies at the heart of warfighting, expanding the influence of technology on our thinking in some cases and entirely replacing the need for humans in others. These are heady topics that any serious professional should be grappling with. Indeed, the very range of the articles in this special issue speaks to the complexity of integrating these key technologies into the profession of arms.

That said, it is impressive to see the talent wrestling with these challenges. On the cyber side, we go from the theoretical underpinnings of policy and foreign affairs in Christina Marcotte's article through the basic definitional grounding provided by Alex Green and Matthew Kellett to the practical reminders of a practitioner in this domain. It is a treat to see these ideas captured in professional writing. On AI, articles in this issue underline the growing influence of the Defence AI Centre, spanning a broad range of

topics and offering practical advice on the implementation of this key technology. The issue also provides an outside view that independently aligns with that vision and its risks.

The topics this special issue challenges us to consider are timely and top of mind. As I write this foreword, I need think back no further than this morning to come up with specific operational examples and recent headlines touching on either AI or cyber security concerns with direct impact on national security and warfighting. Of course, I could have written that statement at almost any time in the past few years, but recent developments have sharpened and accelerated its relevance. We have even seen AI and cyber converge, with models such as Mythos automating the discovery of vulnerabilities in software and contributing to a significant reshaping of the cyber domain.

Therein lies the real reason to engage robustly with the thinking presented in this special issue. We are living through massive shifts in capability brought about by technological advances and witnessing some shockingly rapid shifts in the character of war—even as Ukraine continues to demonstrate its enduring nature as a violent clash of wills. That violence reinforces a central point: the question is no longer whether AI and cyber operations will impact the western way of war, but whether we will react to the ways they already have. This special issue includes a timely and diverse set of perspectives to expand our understanding.

Enjoy.



A G15 Sentinel drone owned by the Advanced Naval Capabilities Unit based in Victoria, British Columbia is parked by the control tent bearing the Canadian Naval Ensign Flag. This drone is used to test interoperability in arctic conditions as part of Operation NANOOK-NUNALIVUT in Inuvik, Northwest Territories on February 27, 2025.

Photo: Master Corporal Alana Morin, Joint Task Force - North, Yellowknife