



The Deck Officer of HMCS MARGARET BROOKE, operates on the bridge as the ship transits to Rothera Research Station, Adelaide Island, Antarctica, during Operation PROJECTION 25-01 on March 15, 2025.

Photo: Corporal Connor Bennett, Canadian Armed Forces Photo

Canada as a Responsible Technology Power in the 21st Century

CHRISTINA MARCOTTE

Christina Marcotte is a deputy director in the International Security Branch at Global Affairs Canada. She spends too much time reading about history and still thinks Vespasian is the most underrated Roman Emperor. The views expressed are her own.

As Canada heads further into the 21st century, I am drawn to the words of 19th century British Prime Minister Lord Palmerston: “We have no eternal allies, and we have no perpetual enemies. Our interests are eternal and perpetual, and those interests it is our duty to follow.”¹

This commentary will describe actions by the Government of Canada (GC) to protect and advance Canadian security interests in an era of technological power. It will focus on cyberspace and cyber tools, including Artificial Intelligence (AI) (for the purposes of this commentary, I will leave aside the presumed

transformative benefits of AI and other technology on business processes). Within this scope, I will focus on the adoption of technology by the state and the governance of its use, both in a responsible way. Responsibility in this context means actions reinforce the international cooperation that has benefitted

Canada and respect Canadian democratic principles. Doing so in these two ways reinforces the governance systems that have allowed Canada and Canadians to prosper.

On the first point, security in the 21st century requires a state to adapt to changing technologies. Without the adaptation, it leaves Canadians exposed to threats to their personal and financial information and leaves Canada at a disadvantage when facing threats from adversary state and non-state actors. Foreign militaries, espionage agencies, criminals, online activists and other malicious actors operate in cyberspace.

With the vast number of threats facing citizens in cyberspace, it would be a violation of the social contract by Canada towards its citizens not to develop and use tools to counter those threats. The social contract includes the agreement that the government will use the money citizens provide to protect them. The capability to act in cyberspace to disrupt and degrade malicious cyber actors, including criminals and the cyber infrastructure criminals use, is part of that protection.²

On the second point, on governance, this is linked to the Rules Based International System (RBIS). The RBIS is the international context that has evolved since WWII and features multilateralism and its institutions such as the United Nations (UN), international law, treaties, and norms.

Canada's economic prosperity is a result of the RBIS providing stable, predictable rules for global trade and economic interactions. At the same time, the RBIS provides Canada with a stable security situation by providing a system to cooperate on international challenges and to develop mutually agreed-to codes of conduct and behaviour. As one of 193 UN member states, and a middle power in a world of increasing numbers of middle powers along with several superpowers, Canada cannot shape the world to its views. Working with like-minded countries is in Canada's interests. The RBIS provides a known and reliable framework for cooperation. It is not perfect, but its underlying values of equality and predictability are far better for Canada than a system where strength alone determines who wins.

In the context of the RBIS, a core pillar of Canada's principles and processes is responsibility. There are two aspects of responsibility. The first is the responsibility to act; the second, to act responsibly. First, those states that can act, should. It is the act of a responsible state to take action when it can. To contest the space where malicious actors operate. To leave the space uncontested leaves citizens vulnerable and at risk, more than they need to be. This is equally true for Canadian citizens as well as citizens of states that lack the wealth and means to take the same actions as Canada can.

Those actions must also be responsible. Canada must use those tools responsibly, in accordance with the RBIS. Specifically, the Framework of Responsible State Behaviour, which Canada publicly committed to at the UN.³ The Framework includes the recognition that international law applies to cyberspace, the adherence and implementation of agreed-to norms (in particular

the 11 UN norms), implementation of cyber-related Confidence Building Measures, and capacity building for developing states⁴.

Using tools responsibly supports and reinforces the RBIS, the same RBIS that has benefitted Canada. This is critical at a time when the RBIS is facing challenges. Real and current challenges from states that are seeking to re-shape the global system to benefit their interests, regardless of the impact on other states, or to benefit from the weakness of other states in a "might makes right" system.

As a democratic country, Canada's responsible state behaviour also includes accountability and transparency. Accountability means Canada adheres to its obligations under applicable international and domestic law, its commitments to voluntary norms and other public commitments, as well as specific, additional governance such as the military chain of command. Transparency means Canada will be public about its capabilities and how it uses them (not including the details of operations) and subject to the appropriate oversight. Both are important to prevent abuse of power and to ensure citizens' confidence in their government.

Turning first to accountability. Technology is used as a tool of state power, which includes AI, whether for espionage, weapons and arms, or other uses not yet foreseen. Yet technology and AI are not separate from the infrastructure that supports it. When I write, "AI will be used as a tool of state power," it also means "AI will be used in cyberspace and as a cyber tool of state power." Cyber is both a domain and a tool. Cyberspace is a domain of civilian and military activity the same as land, sea, air, and space, a place with dimensions through which operations take place. And it is through the RBIS that states worked out how to govern cyberspace. Canada already has clear rules and norms when it comes to cyberspace and using cyber tools, in particular the Framework for Responsible State Behaviour mentioned above. And as AI is integrated into weapons, the use of those weapons will still be governed by rules of engagement and applicable law.

“Canada already has clear rules and norms when it comes to cyberspace and using cyber tools, in particular the Framework for Responsible State Behaviour.”

AI is also more than the next step in cyber, and it is difficult to anticipate all its potential uses. States are aware of this and are currently working within the RBIS to govern how they use AI as a tool of state power. On the military AI side, there are several plural initiatives specific to AI and military use. These include the

2023 United States-led Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy,⁵ which was launched at the Dutch-led Responsible AI in the Military Domain Summit (REAIM 2023). In addition, NATO's 2024 Revised AI Strategy includes an aim specific to responsible behaviour: "to provide a foundation for NATO and Allies to lead by example and encourage the development and use of AI in a responsible manner for Allied defence and security purposes."⁶ On the multilateral side, there is also UN Resolution 79/239 on Artificial Intelligence in the military domain.⁷

Domestically, the Government of Canada is accountable to its citizens for its actions. Actions over the past several years also speak to its credibility as a responsible actor and in meeting its security commitments to its citizens. Actions by the federal government include the publication of a National Cyber Security Strategy in 2018 and in 2024,⁸ the creation of the Canadian Centre for Cyber Security in 2018, the creation of the RCMP's National Cybercrime Coordination Centre, also in 2018, the prevalence of technologies in the Department of National Defence's 2017 Strong, Secure, Engaged,⁹ and 2024 Our North: Strong and Free,¹⁰ and updated legislation for the Communications Security Establishment in 2019.¹¹

Less visible to the public, but equally important was the creation in 2018 of a unit at Global Affairs Canada to focus on cybersecurity policy internationally and which now also includes AI governance. This unit has the expertise required to represent Canada and Canada's security interests at the United Nations and

other multilateral forums and leads on coordinating Canada's contribution to international initiatives such as the United Kingdom- and France-led effort to counter the proliferation of cyber intrusion tools (Pall Mall Process).¹² In addition to this unit, Global Affairs Canada's international law division has lawyers who specialize in cyberspace. This unit contributed meaningfully to the RBIS and to transparency by the Government of Canada by developing and publishing Canada's position on the applicability of international law in cyberspace.¹³

Other measures taken by the Government of Canada for transparency include 2017's Defence strategy Strong, Secure, Engaged, initiative 88, that specifically says the Canadian Armed Forces would "develop the capability to conduct active cyber operations focused on external threats to Canada in the context of government-authorized military missions. The employment of this capability... will be subject to the same rigour as other military uses of force. Cyber operations will be subject to all applicable domestic and international law, and proven checks and balances such as rules of engagement, targeting and collateral damage assessments."¹⁴ Whether those cyber tools are enhanced by AI or not, they will still be subject to accountability mechanisms. By being public about the military's use of active (also called offensive) cyber operations and how they will be governed, Canada reinforces the RBIS.

The *Communications Security Establishment Act* (CSE Act) is also public about Canada's active cyber operations. Section 30



Late in the night, a member of the Canadian Armed Forces sifts through information and data while at the Command Post located at the Maria Montez International Airport in the Dominican Republic 04 May 2024. Nearly 300 members are currently on deployment in the region taking part in an ongoing operation to aid the Canadian embassy in Haiti's capital.

Photo: MCpl Mark Wanzel, Canadian Forces Combat Camera, Canadian Armed Forces

of the CSE Act states that the Ministers of National Defence and Foreign Affairs authorize active cyber operations and subsequent sections of the CSE Act detail the types of activities authorized and prohibited and the procedures for authorization.¹⁵

In addition, from both a democratic principle and transparency perspective, the National Security and Intelligence and Review Agency (NSIRA) and the National Security and Intelligence Committee of Parliamentarians (NSICOP) play key roles. NSIRA's mandate includes the review and investigation of Government of Canada national security and intelligence activities to ensure that they are lawful, reasonable and necessary.¹⁶ Broadly speaking, NSICOP reviews the legislative, regulatory, policy, administrative and financial framework for national security and intelligence and any activity carried out by a department that relates to national security or intelligence.¹⁷ NSIRA and NSICOP must each submit to the Prime Minister an Annual Report, and the Prime Minister tables the Committee's reports in both Houses of Parliament.

On a last note, being a responsible technological actor also gives Canada credibility when increasing cooperation with partners and allies. The scale and scope of the threats mean Canada cannot protect its security alone, and these partnerships are essential. They are essential to understand the threats, develop the best ways to mitigate and manage the threats, and to counter them. Working together takes trust; it takes even more trust to work effectively together. This credibility, from the congruence between Canada's behaviour and its words, helps establish

“Being a responsible technological actor also gives Canada credibility when increasing cooperation with partners and allies.”

Canada as a trusted partner. This includes in longstanding partnerships such as NATO, as well as newly developing and deepening ones as Canada pursues its Indo-Pacific Strategy.

As Canada looks towards the future, as Canada meets its security needs in the years ahead, Canada will continue to be a responsible state player in cyberspace and will be as new technologies are introduced. This includes how Canada will use AI and any other technology as a tool of state power. New technological advancements and the developments associated with them will not change the social contract between Canadians and their government, nor the government's continued work to protect its citizens. The actions taken to date by the GC demonstrate this commitment. Continuing to act as a responsible state player demonstrates the commitment to the governance systems internationally and domestically that have allowed Canadians to prosper.

Notes

- 1 Viscount Palmerston, "Treaty of Adrianople—Charges Against Viscount Palmerston," House of Commons Debates, March 1, 1848, *Hansard*, vol. 97, c. 122. Originally found at: <https://api.parliament.uk/historic-hansard/commons/1848/mar/01/treaty-of-adrianople-charges-against>.
- 2 Jacques J. M. Shore, "An Obligation to Act: Holding Government Accountable for Critical Infrastructure Cyber Security," *International Journal of Intelligence and Counterintelligence* 28, no. 2 (2015): 238. Originally found at: <https://doi.org/10.1080/08850607.2014.962356>.
- 3 Global Affairs Canada, "International Cyber Policy," accessed August 11, 2026. Originally found at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_scurite/cyber_policy-politique_cyberspace.aspx?lang=eng, citing UN General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/70/237 (December 23, 2015).
- 4 UN General Assembly, *Group of Governmental Experts*, A/RES/70/237.
- 5 US Department of State, Bureau of Arms Control, Deterrence, and Stability, *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, November 9, 2023, <https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/>.

- 6 Summary of NATO's Revised Artificial Intelligence (AI) strategy, 5, 11, 10 July 2024. Originally found at: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>
- 7 UN General Assembly, *Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security*, A/RES/79/239 (December 24, 2024).
- 8 Public Safety Canada, *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age* (Government of Canada, June 2018). Originally found at: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrtrg/ntnl-cbr-scrtrg-en.pdf>; Public Safety Canada, *National Cyber Security Strategy: Securing Canada's Digital Future* (Government of Canada, 2025), <https://www.public-safety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrtrg-2025/ntnl-cbr-scrtrg-2025-en.pdf>.
- 9 Department of National Defence, Strong, Secure, Engaged: Canada's Defence Policy (Government of Canada, June 2017). Originally found at: <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html>.
- 10 Department of National Defence, *Our North, Strong and Free: A Renewed Vision for Canada's Defence* (Government of Canada, April 2024). Originally found at: <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html>.

- 11 Communications Security Establishment Act, SC 2019, c 13, s 76. Originally found at: <https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-1.html>.
- 12 United Kingdom, Foreign, Commonwealth & Development Office, *The Pall Mall Process Code of Practice for States* (Government of the United Kingdom, April 4, 2025). Originally found at: <https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states>.
- 13 International Law applicable in cyberspace. Originally found at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_scurite/cyberspace_law-cyberespace_droit.aspx?lang=eng.
- 14 Department of National Defence, Strong, Secure, Engaged, p 73.
- 15 *Communications Security Establishment Act*, s30.
- 16 National Security and Intelligence Review Agency Act, SC 2019. Originally found at: <https://laws-lois.justice.gc.ca/eng/acts/N-16.62/page-1.html>.
- 17 *National Security and Intelligence Committee of Parliamentarians Act*. Originally found at: <https://laws-lois.justice.gc.ca/eng/acts/N-16.61/page-1.html>.