

Preserving Canada's Connected Battlespace Ambitions

by Casey E. Babb

January 2025

POLICY PERSPECTIVE

PRESERVING CANADA'S CONNECTED BATTLESPACE AMBITIONS

by Casey E. Babb

January 2025



Prepared for Triple Helix
Suite 200, 8 York Street, Ottawa, ON K1N 5S6 Canada
www.cgai.ca/triple_helix

©2025 Triple Helix
ISBN: 978-1-77397-327-2

In recent years, scholars, policymakers, military personnel and security officials around the globe have become increasingly concerned about the rapid proliferation of emerging technologies, next generation weapons, and significant changes to the global threat environment. Indeed, Canada's newest Chief of Defence Staff, General Jennie Carignan, said in July 2024 that Canada has "about five years" to adapt, modernize, and prepare for new and emerging threats that could potentially jeopardize our national security.[1] Likewise, former chairman of the joint chiefs of staff, Retired U.S. General Mark Milley recently suggested that we are in the midst of "the most fundamental change" ever in terms of the character of war and conflict.

Yet, despite these pronouncements, repeated calls for change, and largescale strategies to move towards an increasingly digitally dependant military, there remains a dearth of analysis in terms of exploring specific domains, and the potential impacts key advancements and technological capabilities could have on Canada, the U.S., and other allied nations to effectively counter and confront our main adversaries – China and Russia. Two such domains, which are often described as future battlefields for the next generation of warfare, are cyberspace and outer space – areas that while distinct, continue to intersect, complement each other, and create a wide range of both opportunities and potentially disastrous national security vulnerabilities. As a 2023 report from the Centre for International Governance Innovation rather pointedly notes, "there is a volatile 'space-cyber nexus' that commands our urgent attention."

With that in mind, this piece begins with a concise overview of how China and Russia are advancing their cyber and space programs, before mooting several potential steps the Canadian Armed Forces (CAF) and Department of National Defence (DND) could take to ensure these advancements do not jeopardize the country's connected domain ambitions – ambitions which could make the difference between life and death on the battlefield for Canadian and allied servicemembers.

China and Russia: Near-Peer Powers and Ambitious Adversaries

China is actively and aggressively working to become the world's leading spacefaring nation. In fact, in 2022 Beijing publicly stated its goal "to explore the vast cosmos, develop the space industry, and build China into a space power," something the government has described as their "eternal dream."[2] Recent examples highlighting their space ambitions include nearly 70 orbital launches in 2023 – a record for China – as well as their May 2024 Chang'e-6 space mission which for the first time ever, collected samples from the far side of the moon. In addition, Beijing has

[1] Ashley Burke and Darren Major, "New chief of the defence staff says Canada has 5 years to prepare for emerging threats." CBC, July 18, 2024: https://www.cbc.ca/news/politics/new-chief-of-defence-staff-change-in-command-ceremony-1.7266382

[2] China's Space Program: A 2021 Perspective, January 2022: http://english.scio.gov.cn/node_8027953.html#:~:text=%22To%20explore%20the%20vast%20cosmos,outer%20space%20for%20peaceful%20purposes.

made drastic funding increases to the country's space program – up from $3 billion in 2022 to over $19 billion in 2023.[3] That said, China's outer space ambitions go far beyond civil science, research, and exploration; it reflects the fact that Beijing considers their abilities in space to be part of a broader strategic plan to compete with the U.S. and other nations, economically, politically, and crucially – militarily.

For example, China has a range of counterspace weapons at its disposal – weapons which are specifically designed to destroy, degrade and disrupt the space systems much of our critical infrastructure and military assets depend on. In addition to having the ability to physically destroy missiles in Low Earth Orbit, as well as the ability to physically destroy ground-based space infrastructure, China possesses highly sophisticated non-kinetic, electronic, and cyber weapons which can and have proven effective against space assets.[4] Technologies include directed-energy weapons that can, according to the U.S. Director of National Intelligence, "blind or damage sensitive space-based optical sensors, such as those used for remote sensing or missile defense."[5] Likewise, General John Raymond, Commander of SPACECOM and Air Force Space Command stated publicly in 2019, "we're pretty comfortable [in asserting] that they are developing directed energy weapons — probably building lasers to blind our satellites."[6] In early 2020, it was also reported publicly through a state-affiliated academic thesis that China has developed a prototype for an airborne laser weapon, potentially capable of taking down incoming missiles or aircraft.[7] In addition, China possesses advanced satellite jamming capabilities, which the U.S. Department of Defense has suggested is a key component of Beijing's electronic warfare (EW) posture – something China now considers "integral" to modern warfare.[8] Even throughout the COVID-19 pandemic, China continued its space campaign, launching dozens of satellites into space, while also completing the successful operational launch of BeiDou-3 – the country's version of our Global Positioning System (GPS). Underscoring the reality that China's outer space activities pose a considerable threat is the fact that of the more than 700 satellites Beijing has launched and placed in orbit, 245 are for military purposes.

As for the country's cyber capabilities, China has shown its ability to infiltrate satellite systems and take command, hack into organizations responsible for certain satellite operations, and penetrate the networks of firms involved with geospatial imaging technology, big data, and other highly advanced innovations crucial to space dominance.[9] In terms of China's increased blending of cyber and space, the PLA founded the Strategic Support Force to centralize and oversee the

[3] Hema Nadarajah, China: A Global Power's Celestial Ambitions. Asia Pacific Foundation of Canada, May 9, 2024: https://www.asiapacific.ca/publication/china-global-powers-celestial-ambitions
[4] Eric Heginbotham, The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power (1996-2017), RAND Corportation, Santa Monica California, 2015.
[5] *Worldwide Threat Assessment of the U.S. Intelligence Community*, Daniel R. Coats, 2018, pp. 13.
[6] John J. Raymond, (remarks, Mitchell Institute for Aerospace Studies, Washington, DC), reported by Mandy Mayfield, "JUST IN: Space Commander Warns Chinese Lasers Could Blind U.S. Satellites," National Defense Magazine, September 27, 2019, https://www.nationaldefen-tsemagazine.org/articles/2019/9/27/space-commander-warns-chinese-lasers-could-blind-us-satellites.
[7] Minnie Chan, "China's military is hinting at plans for airborne laser attack weapon," Business Insider, January 8, 2020, https://www.businessinsider.com/china-military-hints-at-plans-for-airborne-laser-attack-weapon-2020-1
[8] U.S. Department of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019, 2019, pp. 64.
[9] Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, Tyler Way, and Makena Young, "Space Threat Assessment 2020," Center for Security and International Studies, March, 2020, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/200330_SpaceThreatAssessment20_WEB_FINAL1.pdf?6sNra8FsZ1LbdVj3xY867tUVu0RNHw9V

military's cyber, space and EW operations in 2015 and, in the decade since, analysts suggest China has improved its counterspace cyber arsenal to gain the upper hand during military confrontations. Speaking to this point, the U.S. Defense Intelligence Agency (DIA) stated in their 2019 report, that "China emphasizes offensive cyberspace capabilities as key assets for integrated warfare and could use its cyberwarfare capabilities to support military operations against space-based assets."[10] Striking a similar tone, a 2019 DIA report on China's modernizing military stated that in terms of attacks targeting U.S. satellites, "PLA military writings detail the effectiveness of information operations and cyberwarfare in modern conflicts, and advocate targeting an adversary's C2 and logistics networks to affect the adversary's ability to operate during the early stages of conflict."[11] Moreover, in 2023 a leaked Central Intelligence Agency report suggested that China is developing new cyber weapons designed to "deny, exploit, or hijack" enemy satellites.

All told, China's space program, which is a pillar of nationalistic pride and President Xi Jinping's "Chinese Dream," carries with it immense promise for space exploration, research, and development. However, at the same time, advancements in China's space and cyberspace capabilities also create new pathways for Beijing to exploit critical systems, assets, and infrastructure of Canada and its allies which could end up being the determining factor in a future war.

Unlike China, which has rapidly emerged as a leader in space over the last two or three decades, Russia has maintained its steady position and significant presence in space for the better part of sixty years – despite periods of uncertainty and decline in the country's space program.[12] From launching Sputnik 1 into orbit in October 1957, making first contact with the surface of the Moon in 1959, sending the first human into space in 1961, and Alexei Leonov's spacewalk in 1964, Russia has continually achieved impressive space-related feats – often times before the U.S. and other spacefaring nations. Today, the country maintains one of the world's most significant civil space programs overseen and managed by Roscosmos – Russia's state-run space organization. While companies like SpaceX now possess the capabilities to transport astronauts to and from the International Space Station (ISS), Roscosmos continues to be one of the few organizations in the world with the ability to transport astronauts – as well as supplies – to and from the ISS. With Russia having signed numerous multilateral agreements and treaties regarding the use of space for peaceful purposes, in addition to their international partnerships and collaborative arrangements, Russia has preserved a reputable civil space program, which has been an invaluable foreign policy tool for the Kremlin – particularly during times of conflict.[13]

However, like China, Russia's military and counterspace technologies – including its anti-satellite (ASAT) cyber weapons, are equally, if not more impressive than its civil space advancements. Under the leadership of the Russia Aerospace Forces, Russia has developed advanced

[10] U.S. Defense Intelligence Agency, *Challenges to Security in Space*, 2019, pp. 20.
[11] U.S. Defense Intelligence Agency, China Military Power: Modernizing a Force to Fight and Win, (Washington, DC: 2018), 43, http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf.
[12] Harrison, Johnson, and Roberts, 2019.
[13] Rachel S. Salzman, ""Techno-Diplomacy for the Twenty-First Century: Lessons of U.S.-Soviet Space Cooperation for U.S.-Russian Cooperation in the Arctic," the Carnegie Endowment for International Peace, 2015, https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/Techno-Diplomacy-for-the-Twenty-First-Century-Rachel-Salzman.pdf

counterspace capabilities that have led to concern and consternation throughout the international community. For example, in December 2018, unnamed U.S. officials said Russia had conducted another successful flight test of its new ASAT missile system, the PL-19 Nudol, while in October, 2019, reports surfaced of Russia having tested their new S-500 air defence system in Syria, capable of reaching 300km of orbital altitudes.[14] More recent reports have suggested Russia now possesses physically kinetic ASAT weapons that can "fly practically unlimited distances at very high speeds."[15] In addition, in April 2024, U.S. National Security Advisor Jake Sullivan issued a public statement stating that the U.S. "assesses that Russia is developing a new satellite carrying a nuclear device." In May 2024, U.S. officials also stated that Russia launched a satellite which will likely be used as a counterspace weapon to stalk a U.S. spy satellite. Further, the 2024 Annual Threat Assessment of the U.S. Intelligence Community notes that Russia is "expanding its arsenal of jamming systems, directed energy weapons, on-orbit counterspace capabilities, and ground-based ASAT missiles that are designed to target U.S. and allied satellites."

When it comes to cyber capabilities, Russia is among the most sophisticated countries on Earth. Therefore, it should come as no surprise that they have been increasingly integrating their cyber capabilities with their counterspace efforts. However, relatively little is known about how Russia is blending the domains of space and cyberspace, aside from a small handful of noteworthy cases. For instance, according to analysts at Kaspersky Lab (which itself has been suspected of engaging with the Russian Federal Security Service) a suspected Kremlin-backed hacking group referred to as "Turla", has been hijacking the satellite IP addresses of users to access and obtain data from diplomatic and military agencies in the U.S. and Europe since at least 2007.[16] There are also strong suspicions that Russia jammed GPS signals during NATO exercises in Finland and Norway, while using similar methods of disruption, such as "spoofing" in other locations.[17] In Ukraine, Russia has repeatedly tried to jam and prevent users from accessing Starlink, and it has also been reported that Russia has attempted to disrupt GPS reception in Ukraine and throughout Europe. In fact, Russia's re-invasion of Ukraine in 2022 began with an unprecedented wave of cyber-attacks. To echo one expert – "As the war began, Moscow launched what may have been the world's largest-ever salvo of destructive cyber-attacks against dozens of Ukrainian networks."[18]

All told, Russian military strategists view information superiority as critical to modern warfare and military victory, and cyberspace is a key enabler for Russia in gaining the upper hand in terms of access to, and control of information.[19] In this sense, given the impact of cyberspace through all warfighting domains, and the increasing dependency military technologies now have on space-based assets, cyber-attacks on satellites and other critical space infrastructure could, in theory, give Russia the ability to deny Canada, the U.S., and any other potential adversaries the ability to

[14] Harrison, Johnson, and Roberts, 2019.
[15] Sebastien Roblin, "Russia's Nuclear-Powered 'Skyfall' Missile with Unlimited Range: A Doomsday Weapon?" The National Interest, August 18, 2019.
[16] Center for Advanced Defense Studies (C4ADS), Above Us Only Stars (Washington, DC: March 2019), https://www.c4reports.org/aboveusonlystars
[17] Harrison, Johnson, Roberts, Way, and Young, 2020.
[18] Jon Bateman, Nick Beecroft, and Gavin Wilde, "What the Russian Invasion Reveals About the Future of Cyber Warfare." Carnegie Endowment for International Peace, December 19, 2022: https://carnegieendowment.org/posts/2022/12/what-the-russian-invasion-reveals-about-the-future-of-cyber-warfare?lang=en
[19] Anton Petrov, "Future Warfare," Moscow Defense Brief, no. 3 (2016), http://www.mdb.cast.ru/mdb/3-2016/item1/article1/.

utilize space-enabled information on the battlefield. Going forward, Russia may very well ramp up its cyber operations in space, using them to conduct information warfare at home in support of its national interests and the legitimacy of the Kremlin, while also moulding the decision-making process and calculations of its international rivals, including Canada and the U.S. As many scholarly works and subject matter experts have suggested, Russia, perhaps more than any other actor in cyberspace, has rather successfully devised a way of applying cyber operations and tactics in support of grand scale, strategic objectives – particularly related to the control and manipulation of information. Space architecture, if left unprotected, will serve as another, likely more efficient way of achieving this goal.

Canada, Cyber, and Outer Space: Recommendations for Modernization

Evidently, even a rather cursory overview of hostile state space and cyberspace activities point to the rising dangers these domains pose to Canada. While Canada and its allies look for ways to increasingly integrate space and cyberspace capabilities into their military toolkits while working towards a connected battlespace, countries such as China and Russia are aggressively looking to undermine and exploit these areas.

Therefore, in response to these emerging challenges and potential vulnerabilities, this paper moots a number of recommendations that may contribute to Canada's connected battlespace ambitions, in terms of increasing its awareness of, and abilities to respond to counterspace threats, particularly those connected to cyberspace. It should be noted that the list of recommendations below is not exhaustive, nor are these options mutually exclusive. Furthermore, they should be treated only as an initial, foundational attempt at generating mid to long-term improvements for Canada in these domains.

- Virtually all military engagements depend on space-based infrastructure, and almost all space assets depend on secure cyber technology. These dependencies have given rise to new, and once unforeseen vulnerabilities, capable of derailing mission assurance, and potentially crippling the abilities of forces to detect, prevent, and respond to threats efficiently and effectively. Therefore, given the critical interdependencies of space and cyber assets to military operations, it is recommended that Canada seek out new ways to increase its situational awareness of cyber event related information from across the world – particularly events which could potentially have a nexus to outer space assets. Timely information on cyber attacks, potential points of weakness, and emerging trends, among other things, could be integrated into Canada's decision making, leading to a more comprehensive picture of an all-domain threat landscape. Worth noting, is that in April 2024, Brigadier-General Michael Adamson, the Commander of the Canadian Armed Forces Space Division, said publicly that gaining awareness of what is going on in outer space is one of his top priorities.

- Canada should develop a Centre of Excellence and Expertise for space. Staffed by military personnel, civilian government employees and academics, a centre of this nature would not only serve as a pathway for increased collaboration both inside and outside government, but

it could also increase CAF and DND awareness of emerging space-based threats, including adversarial counterspace cyber capabilities.

- Given China's propensity to use cyberspace as a means to steal their way up the economic, military and intelligence ladder, it is recommended that Canada establish a Blue Ribbon Industrial Advisory Panel to explore ways the country could strengthen its security, by preventing such things as commercial espionage, backdoors in procured equipment, and research agreements with potentially hostile state actors. These and other issues are key concerns related to "research security" – an area the Government of Canada is currently seized with. The Panel would examine everything from homeland defence innovation writ large, to supply chain vulnerabilities, to reliable vendor agreements with private sector companies. Ultimately, the Panel would facilitate enhanced collaboration between the public and private sector, increasing space and cyber resilience, and mitigating vulnerabilities from counterspace cyber-attacks. A panel of this nature comprised of cyber and space experts, with access to Canadian and allied defence practitioners would also help to erode what appears to be a gulf between North American space and cyberspace sectors. To note, a panel of this nature would complement the existing mandate of the Canadian Centre for Cyber Security which is primarily designed to provide expert advice and guidance externally to government, critical infrastructure owners and operators, and the private sector. However, a Blue Ribbon Panel would have the opposite flow of information – with external experts helping the federal government craft strategies to better address some of the issues detailed in this report – issues they so often understand better than government policymakers.

- Canada should also look to take a leadership role not only in designating space assets as critical infrastructure, but in strengthening the resiliency and maintaining the protection of space infrastructure related to military operations. Given the underlying significance of space-based systems to other critical infrastructure and technologies that enable Canadian military capabilities, it would make sense to categorize space assets as critical infrastructure. Designating space systems as critical infrastructure could generate the necessary momentum throughout Canada and abroad to increase government and private sector attention to this vulnerability. As Babb and Wilner have suggested, critical infrastructure protection cannot be addressed in sectoral isolation.[20] Rather, collaborative information sharing agreements, networks and partnerships across sectors such as energy and utilities, information and communication technology, transportation, food, water and space should be facilitated, though designation would be a required first step for space to be sufficiently included.

- Adversaries such as China and Russia are investing heavily in new bleeding edge, breakthrough technologies, in fields such as artificial intelligence (AI) with advancements in subfields like machine, and deep learning. These technologies are being militarized by belligerent nations at a dauntingly unprecedented pace, to the detriment of Canadian and allied military superiority. Should Canada and other allied nations not keep pace, countries

[20] Casey Babb and Alex Wilner, "Passwords, pistols, and power plants: An assessment of physical and digital threats targeting Canada's energy sector," *International Journal*, Vol. 74 (4), 2019.

like China and Russia may eventually secure a technological upper hand in future conflicts, particularly in areas such as cyberspace, and counterspace capabilities. Canada should develop new and innovative ways to leverage domestic expertise in these critically important leap-ahead fields and acquire new technologies, with a view to introduce them into Canada's military operations as quickly as possible.

- Relatedly, Canada should find new ways for academics to work with and conduct research in support of the CAF and DND, particularly in areas related to counterspace capabilities, including cyber, as well as other forms of emerging and disruptive technologies which could prove to be critical for their connected battlespace priorities. Whether it be a standalone conference or symposium on space and cyberspace, fellowships, internships, or grants and scholarships, there are world class experts in both Canada and in other allied nations, whose insights, knowledge and research abilities could be leveraged in support of CAF modernization efforts. Something akin to DND programs like Mobilizing Insights in Defence and Security or Innovation for Defence Excellence and Security would go a very long way in this domain.

Conclusion

These are but a few suggested recommendations intended to generate further thought, not only within the CAF and throughout Canada's security and intelligence community, but amongst academics, policy experts, and defence practitioners throughout Canada and beyond. Ultimately, these and other recommendations should be part of a broader, whole-of-military, and indeed, whole-of-society approach to re-thinking the way Canada must approach conflict in this new age of dual-use technological proliferation and integration. Undeniably, cyberspace and counterspace cyber capabilities are integral elements of both China and Russia's strategies to erode the traditional asymmetric advantages Canada and its allies have had on the battlefield. Lacking attention to these vulnerabilities could lead not only to tectonic shifts in the international balance of power, but in the abilities of Canada to successfully develop a pan-domain force employment concept – something which is both a priority for the military – but also a seriously underappreciated challenge.

About the Author

Dr. Casey Babb *is a senior fellow at the Macdonald-Laurier Institute in Ottawa, an international fellow with the Institute for National Security Studies in Tel Aviv, and a fellow with the Royal United Services Institute in London, England. He's also an advisor to Secure Canada in Toronto, and he teaches courses on terrorism and international security at the Norman Paterson School of International Affairs in Ottawa.*

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.