Hostile State Activity in Cyber and Space: Converging Domains, Future Threats and NORAD's Response

Casey Babb
PhD Candidate
Norman Paterson School of International Affairs
Carleton University
Ottawa, ON
Casey.babb3@carleton.ca

Abstract: In recent years, cyberspace has proven to be an effective and increasingly utilized arena for hostile states looking to carry out attacks, augment their military capabilities, and advance their broader geo-strategic positions. However, after assessing the data, reviewing the literature, and unpacking known and attributable cyber attacks, it becomes clear that two states are behind a significant portion of the most damaging international cyber intrusions. Congruently, these same countries – China and Russia – are aggressively pursuing ambitious space programs. Yet, despite meteoric advancements in both cyber attacks and space programs, little research has been carried out examining the convergence of space and cyberspace, how the two have become interdependent, and how Canadian and U.S. adversaries are strategically advancing their own space and counterspace capabilities to the detriment of North American, and indeed, global security. Therefore, focusing specifically on China and Russia given their technological prowess and near-peer capabilities, this essay explores how each nation is integrating their space and cyberspace efforts militarily, while also suggesting that in light of limited public information on their space programs, patterns of past cyber attacks may be indicative of what future hostile state space operations could look like. Finally, in light of these emerging technological and security challenges, this essay proposes a number of potential foundational recommendations that NORAD could consider as part of a modernization effort to meet the growing demands and threats posed by adversarial advancements in these domains.

Keywords: *cyber, cyber conflict, space, NORAD, modernization*

1. INTRODUCTION

Recently, subject matter experts, practitioners, and defence departments on both sides of the border, have increasingly signalled the need for the North American Aerospace Defense Command (NORAD) to modernize in response to the rapid proliferation of emerging technologies, next generation weapons, and significant changes to the global threat environment.[1] For example, Canada's top military commander stated publicly in March 2020 that the Department of National Defence (DND) had begun work to modernize NORAD in light of new threats, which include, among others, "space-based, aerospace and maritime above and below water."[2] Likewise, speaking before the Senate Armed Services Committee in February 2020, General O'Shaughnessy, Commander of United States Northern Command (USNORTHCOM) and NORAD, said "as we defend the homeland against complex threats in all domains, our commands absolutely understand that the status quo is not acceptable and that we must act now to build a capable defense that provides a credible deterrent."[3] Canada's Prime Minister even mandated the Minister of National Defence to "ensure NORAD is modernized to meet existing and future challenges", as outlined in the country's defence policy.[4] Others, including academics such as Dawson (2019), and Charron and Fergusson (2014; 2015; 2018; 2019) have also called for NORAD to modernize in response to the "multi-domain threat environment".[5]

Yet, despite these pronouncements and repeated calls for change, there remains a dearth of analysis in terms of exploring specific domains, and the potential impacts certain advancements and technological capabilities could have on Canada, the U.S., and NORAD's abilities to effectively protect the continent. 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 potentially disastrous national security and strategic vulnerabilities. As Livingstone and Lewis (2016) have noted, "analysing the intersection between cyber and space security is essential…"[6] if we are to adequately understand and respond to threats emanating from these converging areas.

With that in mind, this essay intends to serve as a primer on the implications and potential threats posed by the blending of cyber and space with an emphasis on counterspace cyber capabilities, while proposing first-step, foundational measures NORAD could pursue to increase its abilities in detecting threats, defeating attacks, and deterring hostile state activities in space and cyberspace. Proceeding in four parts, this essay begins with a succinct overview of how China and Russia are strengthening their space and counterspace cyber capabilities. This section also highlights how certain characteristics of their past cyber attack strategies could – considering limited public information on their space programs – shed light on the future of their counterspace operations. These countries, while not representative of all threat actors concerning NORAD, do account for the two nations that pose the greatest threat to continental security. Furthermore, China and Russia are responsible for a significant portion of the world's most

[1] See: Andrea Charron and James Fergusson, "From NORAD to NOR[A]D: The Future Evolution of North American Defence Co-operation," Canadian Global Affairs Institute, May, 2018; Andrea Charron and James Fergusson, "NORAD: Beyond Modernization," Centre for Defence and Security Studies, University of Manitoba, January 31, 2019; Michael Dawson, "NORAD: Remaining Relevant," Canadian Global Affairs Institute, Vol. 12:39, November, 2019; James Fergusson, "Missed Opportunities: Why Canada's North Warning System is Overdue for an Overhaul," the Macdonald-Laurier Institute, January, 2020; Department of National Defence, "Statement from the Department of National Defence and Canadian Armed Forces regarding NORAD Modernization," National Defence, August 9, 2019;

[2] General Jonathan Vance, remarks delivered at the CDA Institute 2020 Ottawa Conference, March 3, 2020. See: https://cdainstitute.ca/jonathan-vance-speaks-at-2020-ottawa-conference/#

[3] General Terrence J. O'Shaughnessy, statement before the Senate Armed Services Committee, February 13, 2020. See: https://www.armed-services.senate.gov/imo/media/doc/OShaughnessy_02-13-20.pdf

[4] Office of the Prime Minister, "Minister of National Defence Mandate Letter" See: https://pm.gc.ca/en/mandate-letters/2019/12/13/minister-national-defence-mandate-letter

[5] Andrea Charron and James Fergusson, "NORAD: Beyond Modernization," Centre for Defence and Security Studies, University of Manitoba, January 31, 2019

[6] David Livingstone and Patricia Lewis, "Space, the Final Frontier for Cybersecurity?," Chatham House, International Security Department, September, 2016. See: https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf

damaging and disruptive cyber intrusions, making them ideal nations to study in terms of available open-source information and analysis.[7] Following this, we detail the results of our outreach efforts, which were carried out by conducting a social-media campaign, supplemented by an online questionnaire that we distributed widely to a range of subject matter experts throughout academia, government, and the private sector. This approach, while not necessarily ideal in and of itself, was pursued in light of the COVID-19 pandemic, and restrictions related to travel and social distancing, as well as other exogenous factors affecting the likelihood of reaching individuals (e.g. parental responsibilities, changing workplace dynamics, etc.). Next, a number of recommendations are made which, in theory, could potentially lead to a more modern, comprehensive, all-domain mission for NORAD, as well as greater foresight and competence in terms of future space and cyberspace hostilities. In the final section of this paper, we offer brief concluding thoughts and suggestions on where additional research and analysis is needed, as Canada, the U.S., NORAD, our allies, and our adversaries seek to adapt to, and gain the upper hand by blending space and cyberspace capabilities.

2. CHINA AND RUSSIA: NEAR-PEER POWERS AND AMBITIOUS ADVERSARIES

Both China and Russia launched their space programs decades ago, with each having taken aggressive steps in recent years to advance their strategic space and cyberspace operations militarily. In fact, both Chinese and Russian military doctrines suggest they view space as crucial to modern warfare, and according to a 2019 Defense Intelligence Agency (DIA) report, both "view counterspace capabilities as a means to reduce U.S. and allied military effectiveness."[8] With that in mind, the purpose of this section is not to exhaustively unpack the specifics of each country's space and cyber programs, but rather to provide a high-level overview on each country's level of sophistication, achievements, and ambitions in space, with particular attention paid to their counterspace cyber capabilities. Furthermore, given that limited open-source material exists which speaks to the specific capabilities of China and Russia in these domains, I briefly point to certain characteristics of their past cyber attack strategies that could serve as indicators of how their future counterspace operations might evolve, and what their targets and rationale could be driven by.

China: Second only to the U.S. in terms of number of operational satellites, China is – as Drozhashchikh rightfully points out – "rapidly narrowing the gap in quantity and quality of space technologies with global space powers."[9] Since having successfully launched its first satellite in the spring of 1970, China's space program has been marked by a continual string of achievements, many of which have occurred in the last few decades.[10] Ranging from the launch of its manned space program known as Project 921 in 1992, to becoming only the third country ever to achieve independent human spaceflight in 2003, to the successful landing of their "Yutu" rover on the moon in 2013, Beijing has consistently showcased its technological prowess in space.[11] Recent years however, have marked some of China's most significant outer space advancements. For example, in 2016 China launched its Aolong-1 spacecraft with the intent to robotically collect space debris, while in the same year it put the world's first-ever quantum communications satellite into orbit. Remarkably, in 2018 the Middle Kingdom – considered a late bloomer by some in terms of its space program – launched more satellites into space than any country on Earth, with thirty-eight.[12] Furthermore, in January 2019 the country became the world's first to land a spacecraft on the far side of the moon.[13]

[7] Sintia Radu, "China, Russia Biggest Cyber Offenders," U.S.News.com, February 1, 2019; https://www.usnews.com/news/best-countries/articles/2019-02-01/china-and-russia-biggest-cyber-offenders-since-2006-report-shows

[8] U.S. Defense Intelligence Agency, "Challenges to Security in Space", January 2019, pp. 3.

[9] Evgeniia Drozhashchikh, "China's National Space Program and the "China Dream"", *Astropolitics*, 16:3, 2018, pp. 175-186.

[10] United States. Cong. Senate. Statement before the U.S.-China Economic and Security Review Commission "China in Space: A Strategic Competition," April 25, 2019, (Statement of Todd Harrison).

[11] Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, "Space Threat Assessment 2019" (Washington, D.C.: Center for Strategic and International Studies, 2019)

[12] Joan Johnson-Freesearchive, "China launched more rockets into orbit in 2018 than any other country", MIT Technology Review, December 19, 2018; https://www.technologyreview.com/2018/12/19/66274/china-launched-more-rockets-into-orbit-in-2018-than-any-other-country/

[13] Harrison, Johnson, and Roberts, 2019.

However, not all of China's space-related activities are so seemingly benign or civil in nature. In fact, some of the country's most impressive technological abilities in space are their counterspace weapons – weapons designed to destroy, degrade, and disrupt the space systems our critical infrastructure depends on. In addition to having the ability to physically destroy missiles in Low Earth Orbit (LEO), 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.[14] Technologies include directed-energy technology 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."[15] Likewise, General John Raymond, Commander of U.S. Space Command 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."[16] 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.[17] 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.[18] Even throughout 2020, despite facing a global pandemic (COVID-19), China has continued its aggressive space campaign, having launched satellites into orbit in January, February, and as recently as March 24 when they successfully launched three new military surveillance satellites on a Long March 2C rocket.[19] Actions such as this, particularly in light of mounting international scrutiny and attention, speak to how China, and specifically the People's Liberation Army's (PLA), view space as a critical component of modern intelligence gathering and warfare.

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.[20] In terms of China's increased blending of cyber and space, the PLA founded the Strategic Support Force to centralize and oversee the military's cyber, space, and EW operations in 2015 and, in the short time since, analysts suggest China has improved its counterspace cyber arsenal to gain the upper hand during military confrontations. Speaking to this specific point, the U.S. 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."[21] 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."[22] Evidently, China has taken a whole of force approach to future conflict, wherein outer space and cyber space capabilities are integral force multipliers and fields that if harnessed

[14] Eric Heginbotham, The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power (1996-2017), RAND Corportation, Santa Monica California, 2015.

[15] *Worldwide Threat Assessment of the U.S. Intelligence Community*, Daniel R. Coats, 2018, pp. 13.

[16] 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.

[17] 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

[18] U.S. Department of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019, 2019, pp. 64.

[19] Hanneke Weitering, "China's Long March 2C rocket launches military surveillance satellites into orbit", Space.com, Mach 24, 2020; https://www.space.com/china-long-march-2c-yaogan-satellites-launch-success.html

[20] 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

[21] U.S. Defense Intelligence Agency, *Challenges to Security in Space*, 2019, pp. 20.

[22] 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.

effectively, could see China punch above its weight in war. Indeed, China's most recent national defense white paper, released in July 2019, speaks of "outer space, electromagnetic space, and cyberspace" as a single, collective defense aim.[23] Beyond this conjecture though, and given that space has remained relatively peaceful, little is publicly known about China's anti-satellite (ASAT) cyber weapons. However, understanding China's counterspace cyber capabilities may be best understood or predicted by looking at their past behaviour in cyberspace.

When it comes to China's history of cyber attacks, there are certainly consistent characteristics that have defined their strategies in cyberspace, despite the multidimensional tactics they have used in years past. Specifically, with an emphasis on economic and/or commercial espionage through cyber attacks, China has exhibited a sustained prioritization of stealing technical expertise, data, intellectual property, and sensitive technologies from rival nations worldwide.[24] Beijing's activities in cyberspace point to cyber conflict as having broader significance, well beyond the confines of waring and spying, including competition in areas such as the economy, diplomacy, and indigenous technological development and independence.[25] Valeriano, Jensen and Maness (2018) suggest that "China is primarily engaged in cyber espionage that acts to both steal valuable information, altering either its short-term bargaining position or long-term economic and military balance and sending a signal that, as deception or covert action, probes a rival's resolve in a crisis."[26] Furthermore, according to Valeriano, Jensen and Maness, nearly 80 percent of all publicly known cyber intrusions between Beijing and its rivals took the form of cyber espionage.[27] Take for example that recently, numerous sources have reported an uptick in China-backed cyber attacks worldwide, where Beijing-linked hackers have leveraged the COVID-19 pandemic, "exploiting public interest" to again, access, or steal whatever it is they want, from whoever they want it.[28] China has also become increasingly concerned with political and social dissidents, as well as their minority populations, which they have countered and targeted using a range of cyber means, including hacking cell phones, using bots to spread online propaganda, and using social media to coerce and threaten Chinese nationals, at home and abroad.[29] In this sense, China has been able to exploit its 'netizens' and diaspora population's use of the internet to insulate the Chinese Community Party (CCP) and strengthen the regime's political legitimacy and security at home. These two strategies, being indigenous technological development and global technological supremacy, along with shielding the CCP from criticism and dissent, are the main objectives of China's malicious cyber activities, both of which are part of China's efforts to strengthen their position on the battlefield. In line with *Science of Military Strategy*, produced by the PLA, this approach would support what the PLA has discussed in terms of the 'military struggle' in cyberspace, and the necessity for integration of peacetime, and wartime operations.[30] Therefore, given the proliferation of space-based or space-dependent technologies, we might expect to see China find new and innovative ways to exploit the space domain, possibly through cyber attacks, to support these core objectives, in addition to their use of outer space and cyberspace for strategic military purposes. While these are by no means the only ways Beijing has

[23] Li Jiayao, ed., "China's National Defense in the New Era," Ministry of National Defense of the People's Republic of China, Xinhua News Agency, July 24, 2019, http://eng.mod.gov.cn/news/2019-07/24/content_4846443.htm.

[24] James Andrew Lewis, "Emerging Technologies and Managing the Risk of Tech Transfer to China," Center for Strategic and International Studies, September 4, 2019, https://www.csis.org/analysis/emerging-technologies-and-managing-risk-tech-transfer-china; Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation," Defense Innovation Unit Experimental, January 2018, https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf; Alex Joske, "Picking Flowers, Making Honey: the Chinese military's collaboration with foreign universities," Australian Strategic Policy Institute, October 30, 2018, https://www.aspi.org.au/report/picking-flowers-making-honey.

[25] Lyu Jinghua, "What Are China's Cyber Capabilities and Intentions?," Carnegie Endowment for International Peace, April 1, 2019, https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

[26] Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, "Cyber Strategy: The Evolving Character of Power and Coercion," Oxford University Press, 2018, pp. 143.

[27] Valeriano, Jensen, and Maness, 2018.

[28] Zak Doffman, "Chinese Hackers 'Weaponize' Coronavirus Data For New Cyber Attack: Here's What They Did," Forbes, March 12, 2020, https://www.forbes.com/sites/zakdoffman/2020/03/12/chinese-hackers-weaponized-coronavirus-data-to-launch-this-new-cyber-attack/#4dc55f4c3861; Maggie Miller, "Experts report recent increase in Chinese group's cyberattacks," The Hill, March 25, 2020, https://thehill.com/policy/cybersecurity/489531-experts-discover-recent-increase-in-chinese-cyberattacks

[29] Nicole Perlroth, Kate Conger and Paul Mozur, "China Sharpens Hacking To Hound Its Minorities," the New York Times, October 25, 2019.

[30] Zhànlüè Xué, "Science of Military Strategy," Academy of Military Science, Beijing: Military Science Press, 2015.

sought to capitalize on its cyber capabilities, they are integral elements of China's campaign to progressively, and defensively strengthen its position, in advance of future offensive operations in conflict.

Ultimately, China has made rapid and observable progress in space, with no signs of letting up. The country's space program, which is a pillar of nationalistic pride and Xi Jinping's "Chinese Dream", carries with it immense promise for space exploration, research, and development. However, advancements in China's space and cyberspace capabilities also create new pathways for Beijing to exploit the systems and assets of Canada and the U.S., and continue its push for regional and international supremacy in a number of ways, which countries around the world are struggling to combat.

Russia: 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.[31] 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. 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. At present, Roscosmos continues to operate the only launch system transporting astronauts – as well as supplies – to and from the International Space Station, and in 2019, it oversaw and carried out three successful crewed missions into space – two of which are still in progress. 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.[32]

However, like China, Russia's military and counterspace technologies – including its 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 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 defense system in Syria, capable of reaching 300km of orbital altitudes.[33] Other relatively recent reports have suggested Russia now possesses physically kinetic ASAT weapons that can "fly practically unlimited distances at very high speeds"[34] while U.S. analysts have speculated Russia may have new, advanced air-launched ASAT weapons in operational use by 2022.[35] As recent as April 15, 2020, Russia has been testing their direct-ascent ASAT weapons, which the U.S. Space Command said, "provides yet another example that the threats to U.S. and allied space systems are real, serious and growing."[36] Furthermore, Russia also appears to be using outer space as another forum for conducting espionage activities. In a February 2020 interview, U.S. Space Force General John Raymond said in reference to Russian satellite manoeuvres, "this is all circumstantial evidence, but there are a hell of a lot of circumstances that make it look like a known Russian inspection satellite is currently inspecting a known

[31] Harrison, Johnson, and Roberts, 2019.

[32] 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

[33] Harrison, Johnson, and Roberts, 2019.

[34] Sebastien Roblin, "Russia's Nuclear-Powered 'Skyfall' Missile with Unlimited Range: A Doomsday Weapon?" The National Interest, August 18, 2019.

[35] Amanda Macias, "A Never-before-seen Russian Missile Is Identified as an Anti-satellite Weapon and Will Be Ready for Warfare by 2022," CNBC, October 25, 2018, https://www.cnbc.com/2018/10/25/russian-missile-identified-as-anti-satellite-weapon-ready-by-2022.html.

[36] U.S. Space Command Public Affairs, "Russia tests direct-ascent anti-satellite missile," April 15, 2020, https://www.spacecom.mil/MEDIA/NEWS-ARTICLES/Article/2151611/russia-tests-direct-ascent-anti-satellite-missile/

U.S. spy satellite."[37] Russia also possesses the ability to target and successfully impact satellites using non-kinetic, directed energy ASAT weapons, as well as sophisticated EW weapons, which they have used to counter Global Positioning Systems (GPS), tactical communications, satellite communications, and radars.[38] Ultimately, as many observers point out, Russia has continually prioritized and invested in advancing their EW and directed energy weapon (primarily lasers) capabilities which "offer significant potential for military counterspace applications."[39]

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.[40] There are also strong suspicions that Russia has been jamming GPS signals during NATO exercises in Finland and Norway, while using similar methods of disruption, such as "spoofing" in other locations.[41] What we do know though, is that Russian military strategists view information superiority as critical to modern warfare and military victory, and that cyberspace is a key enabler for gaining the upper hand in terms of access to, and control of information. [42] In this sense, given the pervasion 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 utilize space-enabled information in theatre.

Again though, beyond a small handful of publicly known examples, not much is known about Russia's merging of cyber and space, though looking at their history of behaviour in cyberspace may speak to where they are heading in this and other domains. According to Jensen, Valeriano and Maness (2019), Russia's history of cyber attacks suggest that Moscow prefers to manipulate, disrupt, and agitate specific targets and their rivals.[43] Additionally, Jensen, Valeriano and Maness write that Russia tends to use cyber attacks in three distinct ways. First, before a conflict they will use cyber attacks to delegitimize and distract their target. Second, during a conflict they will augment traditional military tactics with cyber attacks, and third, after a conflict they will use cyberspace to disorient their targets, and again, delegitimize them. [44] Similarly, Hodgson (2018) suggests that Russia's cyber attacks are often characterized by coercive objectives, the spread of disinformation, and destabilizing political and social cohesion.[45] Along the same lines, Wirtz (2015) writes that for Russia, cyberspace has been a "key facet of hybrid warfare" and that their "cyber attacks are not specifically targeted to eliminate key nodes, but to intensify the fog of war by sowing confusion within command and control networks."[46] For instance, prior to actual armed conflict in the Russo-Georgian War of 2008, a series of damaging cyber attacks

[37] Sandra Erwin, "Raymond calls out Russia for 'threatening behavior' in outer space," SpaceNews, February 10, 2020, https://spacenews.com/raymond-calls-out-russia-for-threatening-behavior-in-outer-space/

[38] Brian Weeden and Victoria Samson, "Global Counterspace Capabilities: An Open Source Assessment," the Secure World Foundation, April, 2020, https://swfound.org/media/206955/swf_global_counterspace_april2020.pdf

[39] Weeden and Samson, 2020.

[40] Center for Advanced Defense Studies (C4ADS), Above Us Only Stars (Washington, DC: March 2019), https://www.c4reports.org/aboveusonlystars

[41] Harrison, Johnson, Roberts, Way, and Young, 2020.

[42] Anton Petrov, "Future Warfare," Moscow Defense Brief, no. 3 (2016), http://www.mdb.cast.ru/mdb/3-2016/item1/article1/.

[43] Benjamin Jensen, Brandon Valeriano and Ryan Maness, *Fancy bears and digital trolls: Cyber strategy with a Russian twist*, Journal of Strategic Studies, 2019, 42:2, pp. 212-234.

[44] Jensen, Valeriano, and Maness, 2019.

[45] Quentin E. Hodgson, "Understanding and Countering Cyber Coercion", 10th International Conference on Cyber Conflict: CyCon X: Maximising Effects, , ed. T. Minárik, R. Jakschis, and L. Lindström (Tallinn, Estonia: NATO CCD COE Publications, 2018)

[46] James J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," Chaper 3 in Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression Against Ukraine, NATO CCD COE Publications, Tallinn, 2015, https://ccdcoe.org/uploads/2018/10/Ch03_CyberWarinPerspective_Wirtz.pdf

attributed to Russia, hit Georgia's internet infrastructure with millions of distributed denial of service or DDoS attacks shortly before the fighting broke out. At the time, it was the first known incident of a cyberattack coinciding with a shooting war.[47] Again, coinciding with Russia's mobilization into Ukraine, DDoS attacks struck computers in Kyiv, Poland, the European Parliament, and the European Commission. Russia's annexation of Crimea also began with strategic disinformation campaign, confusing Ukraine, delaying their abilities to respond efficiently.[48] Finally (though these examples are not exhaustive), Russia is also known to have carried out wide-ranging cyber espionage and disinformation campaigns in support of the Syrian government.[49] Overall, whether in Ukraine, the U.S., Syria, or elsewhere, Russia has used cyber as a means to carry on the Soviet tradition of political warfare and manipulation in ways we do not see emanating from other countries – at least not on the same scale, or with the same level of sophistication.

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 the U.S. and Canada. As many scholarly works and subject matter experts have suggested before, 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.

3. NORAD, 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 NORAD. While both Canada and the U.S look for ways to increasingly integrate space and cyberspace capabilities into their military toolkits, countries such as China and Russia are aggressively looking to undermine and exploit these areas, derailing the security of the continent, and the collective integrity of NORAD as a whole. Therefore, in response to these emerging challenges and potential vulnerabilities, this paper moots a number of recommendations that may contribute to NORAD's modernization in terms of increasing its awareness of, and abilities to respond to counterspace threats, particularly those connected to cyberspace. However, 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 NORAD in these domains.

- In light of breakthrough technology, particularly hypersonic weapons, which blur the distinction between near space, outer space, and airspace, as well as the fact that Canadian and U.S. adversaries are actively pursuing ways to militarize space, NORAD should develop a distinct space defence mission that complements the existing mission of the U.S. Space Command. Adding space to aerospace warning, aerospace control, and maritime warning could serve as a catalyst for everything from a clear Canadian outer space defence policy, increased Canadian investments in space, and enhanced bilateral research and attention to adversarial counterspace technologies, including cyber, and potential mitigation and defence strategies. The infrastructural pillar of this mission could be a Space Sensing Layer, which General O'Shaughnessy recently suggested is needed to "defend the homeland in all domains."[50]

- 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

[47] John Markoff, "Before the Gunfire, Cyberattacks," the New York Times, August 12, 2008.
[48] Wirtz, 2015.
[49] Sam Jones, "Russia steps up Syria cyber assault," Financial Times, February 19, 2016, https://www.ft.com/content/1e97a43e-d726-11e5-829b-8564e7528e54
[50] General O'Shaughnessy, statement before the Senate Armed Services Committee, February 13, 2020

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 NORAD seek out new ways to increase its situational awareness of cyber event information from both Canada and the U.S. Timely information on cyber attacks, potential points of weakness, and emerging trends, among other things, could be integrated into NORAD decision making, giving NORAD a more comprehensive picture of an all-domain threat landscape. Just as NORAD has been increasing its collaboration with the U.S. Department of Homeland Security, U.S. Cyber Command, and other government partners, Canadian departments and agencies such as the Communications Security Establishment and their new Canadian Centre for Cyber Security, DND, and others, should also be included.

- With funding and participation from both Canada and the U.S., NORAD 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 bilateral cooperation and collaboration on addressing space-based threats, including adversarial counterspace cyber capabilities, it would also strengthen NORAD's internal awareness and expertise, by tapping into world-class policy and research bases on both sides of the border.

- 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 NORAD establish a Blue Ribbon Industrial Advisory Panel to explore ways the alliance could strengthen its security, by preventing such things as commercial espionage, backdoors in procured equipment, and research agreements with potentially hostile state actors. 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 NORAD and the private sector, increasing space and cyber resilience, and mitigating vulnerabilities to counterspace cyber attacks. A panel of this nature comprised of cyber and space experts, with access to Canadian and U.S. policy and defence practitioners would also help to erode what a recent U.S. space executive described as a gulf between North America's space and cyberspace sectors.[51] Increased engagement with the recently created Space Information Sharing and Analysis Center (ISAC) in Colorado may be a first step towards creating a standalone Panel, or perhaps a collaborative agreement with the Space ISAC could be an alternative.

- NORAD, in collaboration with other government departments and agencies in Canada and the U.S., should 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 NORAD's military capabilities, it would make sense to categorize space assets as critical infrastructure. According to Falco (2018), "despite efforts to improve the cybersecurity of critical infrastructure in the U.S., there has been little focus on cybersecurity for space systems."[52] Designating space systems as critical infrastructure could generate the necessary momentum throughout Canada and the U.S. to increase government and private sector attention on this vulnerability. Given NORAD's proximity to the Space ISAC, and the fact the Space ISAC is already "lobbying the Trump Administration to designate commercial space systems as critical national infrastructure", [53] this could be an ideal opportunity to be part of that conversation, and position NORAD as a future guarantor of critical space infrastructure protection. Finally, as Babb and Wilner (2019) suggest, critical infrastructure protection cannot be

[51] Sandra Erwin, "Space executive says the industry needs help to understand cyber threats," Spacenews.com, January 30, 2020, https://spacenews.com/space-executive-says-the-industry-needs-help-to-understand-cyber-threats/

[52] Gregory Falco, "Job One for Space Force: Space Asset Cybersecurity," Harvard Kennedy School Belfer Center for Science and International Affairs, July 12, 2018, https://www.belfercenter.org/publication/job-one-space-force-space-asset-cybersecurity

[53] Shaun Waterman, "Space Industry Seeks Designation as Critical Infrastructure," Air Force Magazine, October 14, 2019, https://www.airforcemag.com/space-industry-seeks-designation-as-critical-infrastructure/

addressed in sectoral isolation.[54] 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 U.S. and allied military superiority. Should the U.S., Canada, and other allied nations not keep pace, countries such as China and Russia may have the technological upper hand in future conflicts, particularly in areas such as cyberspace and counterspace capabilities. NORAD should develop new and innovative ways to leverage American and Canadian expertise in these critically important leap-ahead fields, acquire new technologies, and introduce them into NORAD's military operations as quickly as possible.

- Relatedly, NORAD should look to create new opportunities for U.S. and Canadian academics to work with, and conduct research for the alliance, particularly in areas related to counterspace capabilities, including cyber, as well as other forms of emerging and disruptive technologies. Along the same lines, Charron and Fergusson (2019) have suggested, "NORAD needs, for example, a Canadian NORAD summer school and needs to secure clearances for certain academics to be able to understand and critique the full scope of NORAD challenges."[55] Whether it be a standalone conference or symposium on space and cyberspace, fellowships, internships, grants and scholarships, or something akin to the aforementioned summer school, there are world class experts in both Canada and the U.S., whose insights, knowledge, and research abilities could be leveraged in support of NORAD's modernization.

These are but a few suggested recommendations intended to generate further thought, not only within NORAD, but amongst other academics, policy experts, and defence practitioners throughout Canada, the U.S., and beyond, in terms of steps NORAD could take to meet the rapidly evolving space and counterspace threat environment. Undoubtedly, there is a wide range of very complex political, bureaucratic, and geo-strategic considerations that would need to be taken into account when pursuing most, if not all of these recommendations, and which could very well be at odds with or make implementation of any number of them quite challenging.[56] However, despite these possible impediments, and numerous points of contention between Canada and the U.S., including conflicting views on ballistic missile defence, disparate funding and investment levels between both countries, and differing perspectives regarding the future of outer space in conflict, adversarial advancements in these domains necessitate NORAD, Canada, and the U.S. to pursue innovative solutions.

These and other recommendations, some of which we are hearing for the first time at this Academic Symposium, should be part of a broader, whole-of-military, and indeed, whole-of-society approach to re-thinking the way NORAD, Canada, and the U.S. approach conflict in this new age of dual-use technological proliferation and long-term strategizing. To quote Chris Dougherty, Senior Fellow with the Center for a New American Security, "China and Russia have spent almost two decades studying the current American way of war. While the Department of Defense has taken its military superiority for granted and focused on defeating non-state adversaries, China and Russia have been devising strategies and developing new concepts and weapons to defeat the United States in a war should the need arise."[57] Undeniably, cyberspace and counterspace cyber capabilities are integral elements of both China and Russia's strategies to erode America's traditional asymmetrical advantages on the battlefield.

---

[54] 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.

[55] Charron and Fergusson, 2019, pp. 64.

[56] Charron and Fergusson, in their 2018 paper "From NORAD to NOR[A]D: The Future Evolution of North American Defence Co-operation" cover off many of the most glaring possible obstacles, particularly those related to NORAD undertaking a space defence mission.

[57] Chris M. Dougherty, "Why America Needs a New Way of War," Center for a New American Security, June, 2019, https://s3.amazonaws.com/files.cnas.org/CNAS+Report+-+ANAWOW+-+FINAL2.pdf

Lacking attention to these vulnerabilities could lead not only to tectonic shifts in the international balance of power, but in the abilities of NORAD and USNORTHCOM to successfully meet their objectives and fulfil their responsibilities.

4. CONCLUSION

To recap, countries such as China and Russia, are aggressively pursuing strategies in space with a view to enhance their own abilities, while exploiting the vulnerabilities in allied space and cyberspace architecture. Despite relatively limited public information on the space strategies and abilities of both countries discussed within this paper, ample evidence suggests China and Russia are prioritizing their space and counterspace technologies as part of a broader, comprehensive push to erode U.S. superiority in conflict. Moreover, each country has a lengthy record of carrying out nefarious cyberspace attacks, with patterns and characteristics offering a glimpse of how cyber operations may converge with space-based assets and systems as these technologies continue to evolve, and adversarial strategies become increasingly antagonistic. From China's continual exploitation and theft of big data, technical expertise, IP and sensitive commercial information through cyberspace, to Russia's use of cyberspace for coercion and as a force multiplier for other nefarious military, intelligence, and political operations, it is clear that space and cyberspace are now part of rival nation strategies to achieve supremacy on the battlefield and in other domains related to the military and intelligence supply chain.

As stated in the initial section of this paper, the intent here was to develop an initial primer for Symposium participants on the national security implications of counterspace cyber technologies and space infrastructure vulnerabilities. Therefore, going forward, additional and more comprehensive research will be required which examines everything from what recurring threats are most invasive and damaging, what 'best practices' might look like in the space domain, and how space technologies and architecture will affect cyber conflict in the 2020s and beyond. Furthermore, with other hostile state actors such as North Korea and Iran aggressively seeking to advance their space and counterspace capabilities, as well as their competencies in cyberattacks, additional research should be undertaken analysing what effects any achievements in these domains, emanating from these nations, could mean for NORAD and allied defence. Finally, as others have indicated, additional research should be undertaken analysing the implications of U.S. space-related governance, with the re-establishment of U.S. Space Command and the creation of the new Space Force, and what this will mean for the U.S., Canada, NORAD, and others in terms of outer space security, and who does what, when, where, and how. If we are to sufficiently harden our space infrastructure, increase our chances of military success, and degrade the abilities of our adversaries, these and other questions will need to be addressed, sooner rather than later.