National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Space System Vulnerability Considerations for Future Joint Operational Planning

Major Kimberly Horan

JCSP 48

Service Paper

PCEMI 48

Étude Militaire

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 48 – PCEMI 48
2021 – 2022

Service Paper – Étude militaire

Space System Vulnerability Considerations for Future Joint Operational Planning

Major Kimberly Horan

SPACE SYSTEM VULNERABILITY CONSIDERATIONS FOR FUTURE JOINT OPERATIONAL PLANNING

AIM

1. The space domain is an inherently hostile environment, yet the Canadian Armed Forces (CAF) is increasingly reliant upon it for the conduct of domestic and international operations. The intent of this service paper is to explore the various risks present in space operations, including those generated by state and non-state actors, and how space will affect future CAF, Royal Canadian Air Force (RCAF) or joint expeditionary operations. Additionally, this paper will provide recommendations to the Department of National Defence (DND)/CAF for current and future joint operational planning and as well as future areas for research and development.

INTRODUCTION

2. Many aspects of modern life rely heavily on "space-enabled systems for . . . global communications; environmental monitoring; natural resource management; disaster assistance and mitigation; and weather (terrestrial and space) forecasting." [1] In addition to these, CAF operations also rely upon space-based assets to provide an overall picture of the battlespace; position, navigation, and timing (PNT) information; satellite communications; and intelligence, surveillance and reconnaissance (ISR) data.[2] The First Gulf War was the first time that all of these "space technologies were so highly integrated into strategic, tactical, and operational procedures," and it was an unmitigated success for the United States and their allies, such that space power is now integrated into the doctrine of many western militaries. [3]

3. As described in the United States Space Force inaugural space doctrine, "*military spacepower* [*sic*] is the ability to accomplish strategic and military objectives through the control and exploitation of the space domain." [4] A loss in our ability to exert space power, either through denial, deterrence or deception has the potential for disastrous outcomes on operations. This service paper will explore the various risks that are associated with our reliance upon space assets, and it will consider how these risks might increase in the future as space becomes more accessible to state and non-state actors. This service paper will conclude with a few recommendations for strategic and operational planners to consider based upon the direction of future technology and advancements.

---

[1] Department of National Defence, A-FD-005-001/AF-003, Future Security Environment 2013–2040, 115.

[2]

[3] Cassandra Steer, "Global Commons, Cosmic Commons: Implications of Military and Security Uses of Outer Space," *Georgetown Journal of International Affairs* 18, no. 1 (2017), 11. doi:http://dx.doi.org/10.1353/gia.2017.0003.

[4] United States, *Space Capstone Publication, Spacepower*, 2020), 21.

DISCUSSION

The Space Environment

4. Having established that space power is integral to the CAF, let us now consider what makes up the space domain. For starters, space is not simply defined by a particular altitude above the Earth. A common delineation point when discussing space is the Kármán Line, defined by the Fédération Aéronatique Internationale as 100 km above the mean surface of the Earth, above which the air is too thin to allow traditional aircraft to operate effectively.[5] Most artificial satellites launched into orbit operate at altitudes greater than 200 km to further reduce the effects of drag, as well as to take advantage of specific orbital characteristics, which affect "imagery resolution (fore remote sensing satellites), power required for data transmission, dwell time, and the interval between repeat visits to specific points on the Earth's surface." [6] Without the protection of the Earth's atmosphere, the space environment is harsh, with solar wind and radiation causing damage to sensors, solar panels, and electronic components, degrading capabilities or even disabling the satellite. For this reason, orbiting space systems are hardened to the extent that they can be, and often have several redundancies.

Accidental Collisions

5. Where space was once the purview of superpower nations, expertise within the commercial sector has outstripped governmental departments, while the costs associated with launching satellites have decreased. Accordingly, over the last 20 years we have seen an exponential growth in the number of privately funded organizations investing in space, resulting in an environment that is increasingly congested.[7] Case in point, SpaceX has plans to put more than 12,000 small satellites in orbit to provide global access to space-based commercial internet.[8] Because objects in Earth orbit are subject to much less air resistance than objects such as aircraft, which are sub-orbital, they will continue to persist for a long time, often many years. This increases the probability of incidental contact with other satellites.

6. On 10 February 2009, an American Iridium communications satellite and a defunct Russian Cosmos signals intelligence satellite crashed into each other at a speed of over 10 km/s, the first known collision of two intact satellites, creating a debris cloud of more than 1,600 fragments.[9] The immediate result of this collision - in addition to the

---

[5] "The Karman Line: Where does Space Begin?" last modified 5 March, accessed 20 January, 2022, https://astronomy.com/news/2021/03/the-krmn-line-where-does-space-begin.

[6] Department of National Defence, *Royal Canadian Air Force Doctrine Note 17/01: Space Power* (Ottawa: Department of National Defence, 2017), 7.

[7] Aram Daniel Kerkonian, *Space Regulation in Canada: Past, Present and Potential : The Case for a Comprehensive Canadian Space Law* (Cham: Springer International Publishing AG, 2021), 1.

[8] "SpaceX Fires Off 49 More Starlinks in Rapid-Fire Launch Sequence," last modified 18 January, https://www.cbsnews.com/news/spacex-launch-49-starlink-satellites-rapid-fire-sequence/.

[9] "Russia Destroys Satellite in ASAT Test," last modified 15 November, https://spacenews.com/russia-destroys-satellite-in-asat-test/.

production of space debris, which has more far-reaching consequences - was a signal loss for parts of the Iridium network leaving some customers without access to satellite communications.[10] This blackout lasted a few days until an update patch restored the network.

7. There are currently approximately 42,200 space objects in orbit, of which only 5,300 are active payloads.[11] The Space Surveillance Network (SSN) - consisting of government, university or research institutions, as well as private individuals and organizations - tracks satellites and space debris greater than 10 cm, with the intent to identify any satellite or space vehicle, including the International Space Station (ISS) that is in danger of being struck.[12] Sapphire, a Canadian military satellite built and developed by MDA Canada, contributes to the SSN by tracking objects orbiting at a distance of 6,000 to 40,000 km above the Earth.[13] Satellite operators have one recourse when another space body gets too close; a Collision Avoidance Maneouvre (CAM) fires orbiting thrusters to adjust the heading slightly to ensure that they do not collide, but this uses up fuel.[14] Last year, Europe's Galileo global navigation satellite system completed a CAM to avoid a booster rocket that has been in orbit since 1989.

Anti-Satellite Missiles

8. In addition to accidental collisions between Earth-orbiting satellites, space-based systems are also vulnerable to deliberate actions by adversarial state actors. On 15 November 2021, Russia launched an anti-satellite missile (ASAT), known as the A-235/P-19 Nudol interceptor, destroying another one of its defunct Cosmos satellites.[15] This resulted in a large cloud of space debris, including some 1,500 fragments large enough to be tracked. Shortly thereafter, the expanding cloud of space debris nearly collided with one of the American Defense Meterological Satellite Program weather satellites, responsible for providing weather data in support of military operations. More recently, one of these pieces came within 14.5 metres of a Chinese research satellite, named Tsinghua, passing at a speed of 11,788 miles per hour.[16] At this speed, even small objects have the potential to destroy or disable a satellite.[17]

---

[10] "Iridium Network Patched After Collision in Space," last modified 13 February, https://www.reuters.com/article/technologyNews/idUSTRE51D08B20090214.

[11] "Space-Track.Org," accessed 21 January 2022.

[12] "Backgrounder: Space Situational Awareness and the Sapphire Satellite," accessed 22 January 2022. https://www.canada.ca/en/news/archive/2014/01/space-situational-awareness-sapphire-satellite.html.

[13] *Ibid.*

[14] "EU SST Supports Galileo: First Collision Avoidance Manoeuvre for a Galileo Spacecraft," , accessed 22 January 2022, https://www.eusst.eu/newsroom/eu-sst-supports-galileo-collision-avoidance-manoeuvre/.

[15] "Russian ASAT Debris Imperils DoD, NRO Sats, while ISS Risks Increase: COMSPOC," last modified 4 January 2022. https://breakingdefense.com/2022/01/russian-asat-debris-imperils-dod-nro-sats-while-iss-risks-increase-comspoc/.

[16] "Russian Space Debris Came within 47ft of Knocking Out China Satellite," last modified 21 January 2022. https://www.msn.com/en-us/news/technology/russian-space-debris-came-within-47ft-of-knocking-out-china-satellite/ar-AAT0iIa?ocid=uxbndlbing.

[17] Steer, "Global Commons, Cosmic Commons: Implications of Military and Security Uses of Outer Space," 11.

9. Despite being widely condemned by the international community, this was not the first such demonstration of anti-satellite technology.[18] The United States, Russia, India, and China have also conducted direct-ascent and air-launched ASAT missions in a show of force or as a method to deorbit nonoperational satellites.[19] The 1967 United Nations Outer Space Treaty specifically outlaws space-based nuclear weapons or other weapons of mass destruction (but does not prohibit conventional weapons), while other articles of the treaty state that signatory parties are responsible for the actions of all government or non-government agencies within their territory, including for any damage that is incurred by objects launched into space.[20] This latter aspect of space law has yet to be enforced, yet the Outer Space Treaty remains one of the main deterrence measures against unrestricted aggression within the space domain. To date, only 111 member states have signed and ratified the treaty.[21] While ASAT tests have only thus far been conducted only by space-faring nations who have signed the treaty, future ASAT missions may be carried out by belligerent non-state actors who may be less inclined to adhere to its tenets or to answer to national governments.

Space Operations System

10. While the space segment, that is, the spacecraft itself, is vulnerable to these attacks or mishaps, the remaining two parts of the space operations system, the link segment and the ground segment, are also susceptible.[22] The ground segment comprises the entire ground-based infrastructure, including antennae and operations centres, that are required to "send command signals to satellites for their tasking, telemetry and control." [23] In Canada, responsibility for government space ground segments is shared by the "Canadian Space Agency (CSA), Natural Resources Canada (NRCan), . . . DND, . . . [and] the commercial sector." [24] Ground stations are vulnerable to physical, blunt-force attacks, as well as cyber and electromagnetic spectrum attacks. The link segment:

> comprises the signals in the electromagnetic spectrum that connect the terrestrial segment and the orbital segment. Uplink signals transmit data from Earth to spacecraft. Downlink signals transmit data from a spacecraft to Earth. Crosslink signals transmit data from one spacecraft to another.[25]

Accordingly, it is most vulnerable to cyber attacks.

---

[18] "Russia Destroys Satellite in ASAT Test," last modified 15 November 2021. https://spacenews.com/russia-destroys-satellite-in-asat-test/.

[19] Joan Johnson-Freese and David Burbach, "The Outer Space Treaty and the Weaponization of Space," *Bulletin of the Atomic Scientists* 75, no. 4 (2019), 138.

[20] United Nations, "Treaty on Principles Governing the Activities of States in the Exploration and use of Outer Space, Including the Moon and Other Celestial Bodies," accessed 22 January 2022, https://treaties.unoda.org/t/outer_space.

[21] *Ibid.*

[22] Alexandre Lacasse, telephone conversation with author, 21 January 2022.

[23] Department of National Defence, *Royal Canadian Air Force Doctrine Note 17/01: Space Power*, 9

[24] *Ibid.*

[25] United States, *Space Capstone Publication, Spacepower*, 5.

Cyber Warfare

11. The difficulty with defending space networks against cyber-attack is that "while the cost of attacking in the cyber domain is relatively modest, defending this space is a complex task due to the large number of entry points." [26] By hardening the networks necessary for passing information upstream between the ground and space segments, as well as downstream to the end users, cyber operators reduce the number of vulnerabilities in the overall space system. The number of adversaries capable of conducting cyber-attacks on space networks continues to grow, with states such as Russia and China, as well as organized criminal organizations, activist groups, insurgents, and private citizens conducting a range of cyber operations against a variety of targets for any number of reasons.[27] If networks are unprotected against cyber-attack, "false data or information can be injected . . . allowing adversaries to manipulate the cognitive processes of decision makers and space system operators" resulting in great risk to military operations.[28]

What This Means for Operational Planning

12. All of the vulnerabilities explored thus far, "antisatellite systems, jammers, cyber action, and nuclear threats, place . . . space systems in jeopardy and require serious consideration in operational planning." [29] The Canadian Space Operations Centre (CANSpOC), which falls under Director General Space, who is also the Canadian Space Component Commander (SCC) is an important link to operational commanders by providing Space Domain Awareness (SDA), advice regarding system vulnerabilities and how they might mitigate those.[30] CANSpOC is closely aligned with the Combined Space Operations Center (CSpOC) at Vandenberg Air Force Base, California. "The . . . rapid sharing of information [between these two organizations and their allies] and the . . . conduct of joint missions involving the commercial sector and the intelligence community" ensure greater survivability in the event of any degradation of space-based capabilities.[31] This includes missile warning, critical vulnerability assessments, training, and capacity building.[32]

13. At all stages of the operational planning process (OPP), Commanders and the their staff need to "consider the possibility of hostile actions from both state and non-state actors intent on denying or disrupting friendly forces' use of space capabilities." [33] Greater use of visual planning tools such as synchronization matrixes which integrate space-based capabilities would allow planners to consider:

---

[26] Department of National Defence, A-FD-005-001/AF-003, *Future Security Environment 2013–2040*, 117.

[27] *Ibid.*

[28] United States, *Space Capstone Publication, Spacepower*, 26.

[29] *Ibid.,* 13.

[30] Alexandre Lacasse, telephone conversation with author, 21 January 2022.

[31] James Clay Moltz, "The Changing Dynamics of Twenty-First-Century Space Power," *Journal of Strategic Security* 12, no. 1 (2019) 31. doi:http://dx.doi.org/10.5038/1944-0472.12.1.1729.

[32] Alexandre Lacasse, telephone conversation with author, 21 January 2022.

[33] United States, *Joint Publication 3-14 Space Operations*, 2018), I-7.

> optionality . . . [which] informs the subsequent employment of space systems. In this way, space operations become an integral part of the planning process and contribute[s] to the development of all warfighting function concepts from an early stage. When the operational planner can visualize the array of friendly and enemy forces in time and physical space, vulnerabilities and opportunities become more readily apparent. Anticipating responses to both helps generate options and potential decision points for commanders and staffs" [34]

14. While commanders may not be experts in space or cyberspace, they should at least take every opportunity to employ advisors in these domains. Upon request, CSpOC provides Space Advisors (SA) "to represent Canadian space effects to . . . Coalition partner[s]," and deployable Joint Space Support Teams (JSST), which support the Commander by providing access to space planning tools and space products.[35] The limitations imposed by some host nations mean, however, that the number of deployed personnel on any mission might be inadequate. In all cases, developing a robust deployable and resilient fighting force means training together. While each component is responsible for their own training objectives, certain annual exercises have a joint or even combined component. While the RCAF remains the functional authority for space, the CAF "must have improved interoperability between . . . air, sea, land, space and cyber assets as well as resilient . . . [Command and Control] strategies to enable independent operations in degraded conditions." [36] This requires reaching across Level 1 (L1) organizations to increase awareness of space asset vulnerabilities and to promote training and operational preparedness.

Future Capabilities

15. As the importance of a having a common operating picture of the battlespace only increases, future ISR platforms with increased sensing capabilities will be "placed in polar orbits to allow permanent worldwide ISR collection." [37] Where the adversary has counter-space capabilities such as ASAT missiles or robust cyber capabilities, these would likely be prime targets. As such, militaries such as Canada and its allies will need to be adaptable, prepared to restore access to degraded satellite networks, or in the worst case, launch replacement satellites. Because of this, smaller platforms capable of launching from smaller launch vehicles with short notice "should provide a higher level of resilience in future military and commercial ISR architectures to meet the needs of NATO nations and commanders." [38] This is an area where Canada and the CAF might develop a niche, but it would require even greater cooperation between industry and DND than we currently have.

---

[34] Jerry V. Drew II, "Visualizing the Synchronization of Space Systems in Operational Planning," *Military Review* 99, no. 1 (2019), 113. https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/1318/.

[35] Department of National Defence, *Royal Canadian Air Force Doctrine Note 17/01: Space Power*, 4.

[36] Department of National Defence., *Future Concepts Directive* (Ottawa: National Defence, [2016]).

[37] Tim Vasen, "Responsive Launch of ISR Satellites," *Journal of the Joint Air Power Competence Centre*, no. 27 (2018), 21. https://www.japcc.org/responsive-launch-of-isr-satellites/. (Vasen 2018, 17-27)

[38] *Ibid.*

16. Canada has invested in several upcoming SATCOM initiatives with the United States and other allies, including both Wideband and Narrowband systems, and will in return, will receive bandwidth access to these constellations of communications satellites a significant advantage for deployed operations where traditional communications networks are lacking. [39] While Canada has its own commercial SATCOM capabilities, investing in military networks with our allies ensures interoperability during combined and joint operations, and provides additional redundancy for CAF operations.

CONCLUSION

17. As illustrated above, space is a dangerous and uncertain operating environment, with space-based systems vulnerable to all manner of incidents. Yet, the exploitation of space allows commanders to visualize the battlespace, assess the movements or conditions of their adversary, communicate with their allies, and so much more. Accordingly, "contemporary commanders and [their] staff . . . must consider the space domain as one of many in the employment of operational art with the tactical actions of space systems synchronized in time, multi-domain space, and purpose." [40] Moreover, space power must be a consideration for all current and future operations.

RECOMMENDATIONS

18. Based upon the information presented in this paper, the following are recommendations concerning space vulnerabilities and how they affect current and future CAF joint and combined operations:

a. DND/CAF must continue to partner with the commercial space sector, not just in long-standing partnerships such as MDA Canada, but should also consider investing in small start-ups as proof of concepts for future capability development, including the ability to provide smaller, more flexible space platforms;

b. The CAF must continue to work closely with the United States and our close allied partners and "institutionalize cooperation . . . in space . . . including joint space training, exercises, and operations." [41] International exercises with a major space component should be prioritized, along with national joint exercises, and major training exercises such as the Canadian Army's MAPLE GUARDIAN. These exercises should consider how to operate in a degraded environment, and how to mitigate, including prioritizing, coordinating and sharing informational or bandwidth resources amongst the combined forces; and

---

[39] Moltz, "The Changing Dynamics of Twenty-First-Century Space Power," 30.
[40] Drew, "Visualizing the Synchronization of Space Systems in Operational Planning," 114.
[41] Moltz, "The Changing Dynamics of Twenty-First-Century Space Power," 39.

c. The CAF should consider an establishing an internal strategic governing body to collaborate across L1 organizations and to integrate all space-based considerations for training and operational preparedness.

BIBLIOGRAPHY

Betz, Eric. "The Karman Line: Where does Space Begin?" Accessed 20 January 2022. https://astronomy.com/news/2021/03/the-krmn-line-where-does-space-begin.

Blatt, Talia. "Anti-Satellite Weapons and the Emerging Space Arms Race." *Harvard International Review* 41, no. 3 (2020): 29-34. https://hir.harvard.edu/anti-satellite-weapons-and-the-emerging-space-arms-race/

Bowen, Bleddyn E. "The RAF and Space Doctrine: A Second Century and a Second Space Age." *The RUSI Journal* 163, no. 3 (2018): 58-65. doi:10.1080/03071847.2018.1494349.

Canada. Department of National Defence. "Backgrounder: Space Situational Awareness and the Sapphire Satellite." Accessed 22 January 2022. https://www.canada.ca/en/news/archive/2014/01/space-situational-awareness-sapphire-satellite.html.

Canada. Department of National Defence. *Future Concepts Directive*. Ottawa: National Defence, 2016. http://www.rcaf-arc.forces.gc.ca/en/cf-aerospace-warfare-centre/elibrary/future-concepts-directive-part-2-future-air-operating-concept.page.

Canada. Department of National Defence. *Royal Canadian Air Force Doctrine Note 17/01: Space Power*. Ottawa: Department of National Defence, 2017.

Canada. Department of National Defence. "Space Capabilities." Last modified 13 October 2020. https://rcaf-arc.forces.gc.ca/en/space/capabilities.page.

Chadwick, Johnathon. "Russian Space Debris Came within 47ft of Knocking Out China Satellite." Accessed 21 January, 2022. https://www.msn.com/en-us/news/technology/russian-space-debris-came-within-47ft-of-knocking-out-china-satellite/ar-AAT0iIa?.

Drew, Jerry V., II. "Visualizing the Synchronization of Space Systems in Operational Planning." *Military Review* 99, no. 1 (2019): 106-114. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Jan-Feb-2019/Drew-Space/.

European Union. Space Surveillance and Tracking. "EU SST Supports Galileo: First Collision Avoidance Manoeuvre for a Galileo Spacecraft." . Accessed 22 January, 2022. https://www.eusst.eu/newsroom/eu-sst-supports-galileo-collision-avoidance-manoeuvre/.

Foust, Jeff. "Russia Destroys Satellite in ASAT Test." https://spacenews.com/russia-destroys-satellite-in-asat-test/.

Harwood, William. "SpaceX Fires Off 49 More Starlinks in Rapid-Fire Launch Sequence." . https://www.cbsnews.com/news/spacex-launch-49-starlink-satellites-rapid-fire-sequence/.

Hitchens, Theresa. "Russian ASAT Debris Imperils DoD, NRO Sats, while ISS Risks Increase: COMSPOC." https://breakingdefense.com/2022/01/russian-asat-debris-imperils-dod-nro-sats-while-iss-risks-increase-comspoc/.

Johnson-Freese, Joan and David Burbach. "The Outer Space Treaty and the Weaponization of Space." *Bulletin of the Atomic Scientists* 75, no. 4 (2019): 137-141. https://www.tandfonline.com/doi/abs/10.1080/00963402.2019.1628458?

Kerkonian, Aram Daniel. *Space Regulation in Canada: Past, Present and Potential : The Case for a Comprehensive Canadian Space Law*. Cham: Springer International Publishing AG, 2021. https://link.springer.com/book/10.1007/978-3-030-68692-5.

Moltz, James Clay. "The Changing Dynamics of Twenty-First-Century Space Power." *Journal of Strategic Security* 12, no. 1 (2019): 15-43. doi:http://dx.doi.org/10.5038/1944-0472.12.1.1729.

Nordquist, Keith B., USAF. "The New Matrix of War." *Air & Space Power Journal* 32, no. 1 (2018): 109-117. https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-30_Issue-2/2018_2_08_nordquist_s_eng.pdf

Steer, Cassandra. "Global Commons, Cosmic Commons: Implications of Military and Security Uses of Outer Space." *Georgetown Journal of International Affairs* 18, no. 1 (2017): 9-16. doi:http://dx.doi.org/10.1353/gia.2017.0003.

Thompson, David "D T", USAF, Gregory J. Gagnon USAF, and Christopher W. McLeod USAF. "Space as a War-Fighting Domain." *Air & Space Power Journal* 32, no. 2 (2018): 4-8. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-32_Issue-2/SLP-Thompson.pdf.

United States. Department of Defense. *Joint Publication 3-14 Space Operations,* 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14ch1.pdf.

United States. Department of Defense. *Space Capstone Publication, Spacepower,* 2020. https://www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf.

Untied Nations. Office for Disarmament Affairs. "Treaty on Principles Governing the Activities of States in the Exploration and use of Outer Space, Including the Moon and Other Celestial Bodies." Accessed 22 January 2022. https://treaties.unoda.org/t/outer_space.

USSPACECOM. "Space-Track.Org." Accessed 21 January 2022.

Vasen, Tim. "Responsive Launch of ISR Satellites." *Journal of the Joint Air Power Competence Centre* no. 27 (2018): 17-27. https://www.japcc.org/responsive-launch-of-isr-satellites/.

Wolf, Jim. "Iridium Network Patched After Collision in Space." Last modified 13 February 2009. https://www.reuters.com/article/technologyNews/idUSTRE51D08B20090214.