National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Entry Denied: Future Warfare in an Anti-Access Area Denial Theatre

Major Richard Hough

JCSP 50

Exercise Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI n° 50

Exercice Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 50 - PCEMI n° 50
2023 - 2024

Exercise Solo Flight – Exercice Solo Flight

Entry Denied: Future Warfare in an Anti-Access Area Denial Theatre

Major Richard Hough

ENTRY DENIED:
FUTURE WARFARE IN AN ANTI-ACCESS AREA DENIAL THEATRE

INTRODUCTION

In the not-too-distant future, a rogue state has decided to challenge Western legitimacy in the Pacific region. As pro-western states respond militarily, the rogue nation takes control of vital terrain. While attempting to take it back, Western forces notice some concerning effects: ships appear to be navigating on land, ghost vessels appear on navigation displays, communications are sporadic and, for some reason, all their intelligence gathering satellites become inoperable as they traverse the region of interest. The regional commander is concerned that the adversary is attempting to create an anti-access/area denial (A2AD) region in this theatre. They have concerns, but due to pre-mission preparation are ready to respond to these types of threats and still complete their assigned mission.

Recent conflicts where the Canadian Armed Forces (CAF) have been involved have taken place in a relatively permissive environment. While Afghanistan, Libya, and Iraq all had adversary actions, the adversary's ability to deny regions to allied forces was limited. The same should not be expected in future conflicts, in any domain. A future conflict with either a peer or near-peer adversary can be expected to have an aspect of A2AD. A working NATO definition of A2AD strategy is "to prevent the attacker from bringing its forces into the contested region (A2) or to prevent the attacker from freely operating within the region and maximizing it combat power (AD)."[1]

While the scenario above is fictional, it demonstrates how a future conflict in an A2AD environment could unfold. While it is desirable to examine all potential scenarios, this paper will only look at the aspects of space denial, stealth and electronic warfare (EW). Other A2AD techniques, such as weapons systems and their associated warning systems will not be covered as discussion of these items will rapidly enter the classified realm. This does not mean that discussions of space, stealth and EW do not have secret aspects, however, there is significantly more research available at the unclassified level. The paper will explore a few methods that an A2AD region could be created, including whether Russia and China may utilize or support use of such techniques.

---

[1] LCol Andreas Schmidt. "Countering Anti-Access/Area Denial." *Transforming Joint Air Power: The Journal of the JAPCC*. No 23 (Autumn/Winter 2016): 70. https://www.japcc.org/wp-content/uploads/JAPCC_Journal_Ed-23.pdf

SPACE DENIAL

Space can be thought of as the ultimate high ground in any combat scenario. It can also be a critical enabler to operations in all the other domains, making Space the definitive joint warfighting domain. Operations on Land, at Sea and in the Air depend on space assets, and therefore space control for things such as communications, navigation, targeting, intelligence gathering and timing is essential. If these can be disrupted in a region, an A2AD scenario will play out. Damaging or destroying satellites in orbit, or during launch is one of the things that concerns the US military in a future conflict.[2]

Space assets may be vulnerable in a near-peer sponsored conflict due to the challenge in directly protecting satellites. In a future conflict, three methods of denying access to these satellites include: jamming of uplink and downlink signals, physical destruction of the satellites and rendering satellites inoperative by ruining their electronic components. For this paper, we will examine the later two options as techniques a rogue nation could use to create an A2AD scenario and to attempt to gain advantage over Western forces. The degradation and / or destruction of satellites would have an influence on allied operations due to the potential loss of communications, navigation and intelligence gathering assets. Loss of these systems could make attacking a rogue nation more difficult as Western nations depend on these systems. There would be a resulting performance increase in defensive systems which do not depend as heavily on technology. It could be expected that a rogue nation may not have the ability to surgically select space assets for destruction, and would use techniques to deny in a wider fashion. "Russia may face significant challenges with its space awareness and still cannot claim to have complete counter-space EW capabilities."[3] As such, Russia may need to be considered similarly to a rogue nation when it comes to counter-space capability.

Nuclear Space Denial

The first method to deny access to space assets could be for a rogue nation to detonate a nuclear weapon in space, creating an electromagnetic pulse (EMP).[4] As demonstrated in the 1962 STARFISH PRIME tests by the US, along with others conducted by the Soviet Union, high-altitude detonations of a nuclear payload can have immediate and long-lasting effects on satellites. While these effects will be primarily

---

[2] Eric Berger. "The US military just proved it can get satellites into space super fast." Updated September 15, 2023. https://arstechnica.com/space/2023/09/firefly-and-space-force-demonstrate-ability-to-rapidly-launch-a-satellite/

[3] Pavel Luzin. "Electronic Warfare: Russia's approach." *Foreign Policy Research Institute: Eurasia Program.* February 2022: 14. https://www.fpri.org/wp-content/uploads/2022/02/electronic-warfare-022222.pdf

[4] E. Conrad *et al*. "Collateral Damage to Satellites from an EMP Attack." (Fort Belvoir, VA: Defence Threat Reduction Agency, August 2010), 30. https://apps.dtic.mil/sti/pdfs/ADA531197.pdf

limited to low Earth orbiting satellites (unless a significant yield payload is used), many different satellite systems which are used for military operations will be affected.[5] Loss of low Earth satellites would have an impact on military operations due to the loss of some communications satellites (e.g. ,IRIDIUM, Starlink), and intelligence gathering satellites (including weather satellites used for mission planning).[6] Satellites at higher altitudes, including geostationary communications satellites and navigation satellites are less likely to be affected by detonations of this type which have less than multi-megaton yields.[7] "A nuclear detonation in space would add significant radiation to orbits… causing them to degrade in the weeks and months following the detonation unless they are specifically hardened against radiation."[8] According to a current member of US Space Command, not all military communications are done through military satellites.[9] Military activities which are done through commercial satellites would be at higher risk to disruption as commercial satellites tend to have lower levels of protection against a high energy event such as a high-altitude EMP.[10]

Concerns have recently been expressed by the White House about reports that the Russians may be ready to place an anti-satellite system into orbit.[11] Although US media report that the weapon could be of the nuclear variety, this has not been confirmed by official sources. This sort of system could be either used as described above to create an EMP, or it could be used as a power source for an EW jamming type weapon. Due to the distance satellites are from control stations, or users, they frequently have sensitive receiving systems to obtain their signals of interest. The power created by a nuclear-powered jamming system could cause significant, long-term degradation to communications with satellites in the region.[12] This could help create a region of A2AD.

---

[5] *Ibid.* i.

[6] Kateryna Sergieieva. "Types of Satellites: Different Orbits & Real-World Uses". *EOS Data Analytics* (blog), 22 March 2023, https://eos.com/blog/types-of-satellites/

[7] E. Conrad *et al*. "Collateral Damage to Satellites…" 5.

[8] Clementine Starling and Mark Massa. "Russian nuclear anti-satellite weapons would require a firm US response, not hysteria." *New Atlanticist*. 15 February 2024. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-nuclear-anti-satellite-weapons-would-require-a-firm-us-response-not-hysteria/#:~:text=It%20follows%20that%20an%20adversary,by%20destroying%20their%20own%20satellites.

[9] Aaron Hines. Email to author dated 10 April 2024.

[10] E. Conrad *et al.* "Collateral Damage to Satellites…" 4.

[11] The Associated Press. "White House confirms reports of Russia's 'troubling' anti-satellite weapon capability" updated 15 February 2024. https://www.cbc.ca/news/world/white-hours-russia-space-weapon-1.7116704

[12] "How much damage could a Russian nuclear space weapon do?" About That video, 10:14. posted by "CBC," 5 March 2024. https://www.cbc.ca/player/play/1.7134389

Conventional Direct Attack Weapons

Another method which an adversary could use to attack space assets would be a conventional ground to space launch. This could be done in one of two different ways. The first would be a direct launch against a specific satellite with a missile with the goal of striking and destroying the target satellite. This capability has been demonstrated by four countries: USA (1985), India (2007), China (2007) and Russia (2021).[13] While seemingly simple, an attack in this manner is reasonably complex due to the speed that both the satellite and the anti-satellite weapon are travelling. A secondary effect of a successful intercept is that the targeted satellite and interceptor missile will create a cloud of debris, which will spread out, as was seen after the Chinese anti-satellite test, which may result in other satellites being impacted due to an increase in space debris.[14]

This leads to the second conventional technique which could be used to render a region of space unusable. This technique would be to detonate a weapon in space that has the only goal of increasing the amount of space debris in a specific orbit. There would be no requirement to directly impact another satellite. The result of this increased amount of debris could cause the Kessler Effect, where there is a cascading number of collisions as active satellites impact debris – creating more debris, which impact active satellites, etc. rendering certain orbits, or orbital regions unusable.[15]

While this type of attack, like the EMP attack previously described, would be indiscriminate, a rogue nation who did not depend on satellite technology to prosecute military actions could use this to great effect against a nation who did depend on these services. Defences against this type of denial include: timely satellite manoeuvres (works against the first type of attack, but reduces satellite lifespan), increased armour (increased cost to launch) and work to remove space debris which is already in existence. While cleaning up orbital debris has been suggested as an option to pro-actively protect satellites currently in orbit, there are those who propose that the removal of debris may actually have a detrimental effect on discouraging the use of direct-kill anti-satellite weapons.[16]

---

[13] Clementine and Massa. “Russian nuclear anti-satellite…”

[14] Shirley Kan. “China’s Anti-Satellite Weapon Test.” *CRS Report for Congress*. 23 April 2007. https://apps.dtic.mil/sti/pdfs/ADA468025.pdf

[15] B. Mrusek and L. Weiland, "Space Commercialization and the Rise of Constellations: The Resulting Impact on the Kessler Effect," *2023 IEEE Aerospace Conference*, (Big Sky, MT, USA, 2023): 1. doi: 10.1109/AERO55745.2023.10115734.

[16] Gregory Miller. “Deterrence by Debris: The Downside to Cleaning up Space.” *Space Policy* 58, (November 2021): 3. https://www.sciencedirect.com/science/article/pii/S0265964621000394?via%3Dihub

Navigation Warfare

A third method for creating an A2AD region through disruption of space assets would be a disruption of navigation and timing signals found on the Global Positioning Satellite system (GPS). This concept is not a new one and was observed during the 1991 Persian Gulf War when a jamming signal was put around Saddam Hussein's palaces as protection.[17] There is an increased threat of GPS, with foreign nations finding new ways to manipulate the GPS timing signal, resulting in inaccurate positions to the end users. Ships operating in Chinese waters have observed their positions changing and their ship appearing to be periodically positioned over land.[18] In Russia, it has been observed that GPS signals are inaccurate in areas where President Vladmir Putin is operating. Unlike the Chinese technique which slightly displaces user positions, the Russians use a technique which places all nearby receivers virtually to the same distant location.[19] Both of these techniques could be used in an area denial situation, and cause issues with both targeting and navigation, potentially providing an additional propaganda tool for the adversary should a missile strike a prohibited target, or a military ship cause ecological damage due to a navigational error.

While this threat is real, and has been for a while, NATO and the US have recognized the threat and have been working on solutions. NATO has developed a tool which will allow planners to estimate where GPS jamming will be effective so that they can adjust their tactics and plans.[20] To make jamming more difficult, the US have been launching new satellites which provide a stronger military signal. Currently, sufficient satellites have been launched to provide this new code to military users, however, there is still an issue with end users having the correct receivers to take advantage of this modification. Looking further to the future, the US Air Force (owners of the GPS system) is looking to have the next generation of satellite-based navigation system to have the system be reprogrammable so that different encryption and frequencies can be used when an attack is discovered.[21] Until these US system modifications are realized, there remains the solution that was realized during the 1991 Persian Gulf War: when GPS is

---

[17] Larry Greenemeier. GPS and the World's First "Space War". *Scientific American.* Updated 8 February 2016. https://www.scientificamerican.com/article/gps-and-the-world-s-first-space-war/#:~:text=GPS%20jamming,from%20being%20hit%2C%20Mastalir%20says.

[18] Dana Goward. "Patterns of GPS Spoofing at Chinese Ports." *The Maritime Executive*. 19 December 2019. https://maritime-executive.com/editorials/patterns-of-gps-spoofing-at-chinese-ports

[19] C4ADS. "Above us only stars". 26 March 2019. https://c4ads.org/reports/above-us-only-stars/

[20] Nathan Strout. "NATO's new tool shows the impact of GPS jammers." *Defence News*. Updated 15 April 2020. https://www.defensenews.com/newsletters/military-space-report/2020/04/15/natos-new-tool-shows-the-impact-of-gps-jammers/

[21] Sandra Erwin. "U.S. military doubles down on GPS despite vulnerabilities." *Space News*. 9 August 2021. https://spacenews.com/u-s-military-doubles-down-on-gps-despite-vulnerabilities/

unavailable, use laser guided munitions to keep collateral damage to an acceptable level.[22]

When assessing the risk of attacking space assets, both an EMP type attack and a Kessler Syndrome type attack would be indiscriminate attacks on satellite systems. It can be presumed that a peer adversary who depends on space for their own military operations would not use these types of attacks to create and A2AD environment. The same cannot be said about a rogue nation. To counter the loss of satellite data, the US has investigated the ability to quickly launch replacement satellites. During trials in the early 2020's, they demonstrated the ability to have a satellite "launch ready" from a storage condition to orbit in 27 hours. Additionally, they built a satellite from available components and launched it into space within 21 days.[23] While this would leave a period where forces were unable to use space assets, it demonstrates that satellite destruction may not be as critical as once believed. Attacking the GPS constellation may be restricted to a more regional attack, however; the adversary may also decide to use one of the destruction techniques, risking their global standing due to the disruptions.

---

[22] Larry Greenemeier. GPS and the World's First "Space War". (2016)

[23] Eric Berger. "The US military just proved it can get satellites into space super fast." Updated September 15, 2023. https://arstechnica.com/space/2023/09/firefly-and-space-force-demonstrate-ability-to-rapidly-launch-a-satellite/

THE PROMISE OF STEALTH

A terrestrial method of creating an A2AD region is to create a fence of detectors which are linked to numerous weapons systems to target any threats crossing into the defended area. From an air perspective, this is frequently called an Integrated Air Defence System (IADS), for the Navy, it may include a line of sonar detection systems coordinated with shoreline radars. While there may not be a direct analog for the Army, they would require the assistance from one of the other two services to get into theatre so would be operationally impacted similarly. To defeat these types of detection systems, the concept of stealth continues to be developed.

While the Army has been practicing stealth for generations, through camouflage and concealment practices, it is a more recent development for the Air Force and Navy. Each of the services are also concerned with different portions of the electromagnetic (EM) spectrum. The Army concerns itself primarily with visible spectrum, the Air Force with radar and the Navy with acoustic signatures (although they do have some concerns in radar frequencies too). Each service also has some concerns in the infra-red (IR) or heat portion of the spectrum.

Radar stealth for aircraft is frequently seen by the public as an essential piece of new acquisitions. While this may be the case, adversaries have also developed their own stealth platforms. Head-to-head capabilities between western and Russian (or Chinese) stealth aircraft is classified. However, this is not the only way that our potential adversaries are preparing to combat stealth aircraft. As was demonstrated over Yugoslavia, even stealth aircraft can be detected and shot down if the conditions are correct.[24] Most low observable aircraft are designed to function against X-Band radars from a frontal aspect, so modifying these conditions by using a different frequency band, or through the use of multi-static radars may make stealthy aircraft vulnerable to attack.[25] This type of tactical adaptation should be expected from the adversary. Some of the adjustments may be observable pre-mission, however other tactical modifications will only be noticed during or post-mission. Allied tactics would need to remain flexible.

ELECTRONIC WARFARE

Both of our main potential adversaries, Russia and China, have recognized the value of EW in the future fight, and are adjusting their forces to be able to function in this

---

[24] Andrew Metrick. "A Cold War legacy: the decline of stealth". *War on the Rocks*. Updated 20 January 2015. https://warontherocks.com/2015/01/a-cold-war-legacy-the-decline-of-stealth/

[25] Brigadier Arvind Dhananjayan. "Countering Stealth Technology in Military Aviation." *Indian Defence Review* 38.1 (Jan-Mar 2023). https://www.indiandefencereview.com/news/countering-stealth-technology-in-military-aviation/

environment. Russia has been assessed to rely on A2AD systems, including EW and other forms of asymmetric warfare measures due to their inability to develop their armed forces in the same way as Western nations.[26] China has been working on improving their own EW systems since the 1930s, making statements like "fighting for supremacy in the electromagnetic spectrum has become key to success or failure in war" and "Outer space will be the primary domain for the forward march of electronic warfare."[27] The use of EW to create A2AD regions can be expected from both of these adversaries, along with other kinetic/missile systems.

[26] Pavel Luzin. "Electronic Warfare: Russia's approach."6.

[27] Shaoxing Xu. "Electronic Warfare in China's Past, Present, and Future". Last modified 29 November 1995: 7. apps.dtic.mil/sti/citations/ADA304506

CONCLUSION

The concept of A2AD is not a new one in warfare, however, the methods being used to create these regions are new. Historically, walled cities denied raiders access to valuable resources, moats protected castles and barrage balloons during World War 2 attempted to prevent allied aircraft from entering regions. All of these can be considered pre-cursor A2AD systems. In the current and future combat environment, these A2AD systems are more likely to have a technology aspect to them, as demonstrated through the discussion of space denial, stealth and electronic warfare. While some of the allied forces are more adept at working in a low-tech environment, each of the major domains (Land, Air, Sea) regularly train for operations where technology has been denied by the adversary. This demonstrates a willingness to recognize the threat, and to develop ways to counter or protect one's forces should A2AD techniques be employed in combat. Given the technological nature that these systems now focus on, the challenge becomes one of keeping up or ahead of the adversary to maintain combat advantage. Since the adversary also continues to develop their systems, the determination of a winner in this race may not be known until a future major powers conflict.

BIBLIOGRAPHY

Associated Press, the. "White House confirms reports of Russia's 'troubling' anti-satellite weapon capability" updated 15 February 2024. https://www.cbc.ca/news/world/white-hours-russia-space-weapon-1.7116704

Berger, Eric. "The US military just proved it can get satellites into space super fast." Updated September 15, 2023. https://arstechnica.com/space/2023/09/firefly-and-space-force-demonstrate-ability-to-rapidly-launch-a-satellite/

C4ADS. "Above us only stars". 26 March 2019. https://c4ads.org/reports/above-us-only-stars/

Clark, Bryan. "The Fall and Rise of Russian Electronic Warfare." *IEEE Spectrum.* 30 July 2022. Spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare

Conrad, E., G. Gurtman, G. Kweder, M. Mandell, and W. White. "Collateral Damage to Satellites from an EMP Attack." Fort Belvoir, VA: Defence Threat Reduction Agency, August 2010. https://apps.dtic.mil/sti/pdfs/ADA531197.pdf

Dhananjayan, Brigadier Arvind. "Countering Stealth Technology in Military Aviation." *Indian Defence Review* 38.1 (Jan-Mar 2023). https://www.indiandefencereview.com/news/countering-stealth-technology-in-military-aviation/

Erwin, Sandra. "U.S. military doubles down on GPS despite vulnerabilities." *Space News*. 9 August 2021. https://spacenews.com/u-s-military-doubles-down-on-gps-despite-vulnerabilities/

Goward, Dana. "Patterns of GPS Spoofing at Chinese Ports." *The Maritime Executive*. 19 December 2019. https://maritime-executive.com/editorials/patterns-of-gps-spoofing-at-chinese-ports

Greenemeier, Larry. "GPS and the World's First 'Space War'." *Scientific American.* Updated 8 February 2016. https://www.scientificamerican.com/article/gps-and-the-world-s-first-space-war.

Harris, Mark. "Ghost ships, crop circles, and soft gold: A GPS mystery in Shanghai." *MIT Technology Review*. 15 November 2019. https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/

"How much damage could a Russian nuclear space weapon do?" About That video, 10:14. posted by "CBC," 5 March 2024. https://www.cbc.ca/player/play/1.7134389

Kan, Shirley. “China’s Anti-Satellite Weapon Test.” *CRS Report for Congress.* 23 April 2007. https://apps.dtic.mil/sti/pdfs/ADA468025.pdf

Knowles, J. "A2AD Threats Shifting NATO EW Focus." *Journal of Electronic Defense* 39, no. 6 (2016): 24

Luzin, Pavel. “Electronic Warfare: Russia’s approach.” *Foreign Policy Research Institute: Eurasia Program.* February 2022. https://www.fpri.org/wp-content/uploads/2022/02/electronic-warfare-022222.pdf

Metrick, Andrew. “A Cold War Legacy: The Decline of Stealth.” *War on the Rocks.* 20 January 2015. https://warontherocks.com/2015/01/a-cold-war-legacy-the-decline-of-stealth/

Miller, Gregory. “Deterrence by Debris: The Downside to Cleaning up Space.” *Space Policy* 58, (November 2021): 3. https://www.sciencedirect.com/science/article/pii/S0265964621000394?via%3Dihub

Mrusek, B. and L. Weiland, "Space Commercialization and the Rise of Constellations: The Resulting Impact on the Kessler Effect," *2023 IEEE Aerospace Conference*, Big Sky, MT, USA, 2023, pp. 01-07, doi:10.1109/AERO55745.2023.10115734.

Prisha (ed.) “China reveals new generation electronic warfare weapon.” Updated 2 January 2024. https://www.wionews.com/world/china-reveals-new-generation-electronic-warfare-weapon-heres-how-it-threatens-the-world-675796

Schmidt, Andreas. “Countering Anti-Access/Area Denial.” *Transforming Joint Air Power: The Journal of the JAPCC.* No 23 (Autumn/Winter 2016): 69 – 77. https://www.japcc.org/wp-content/uploads/JAPCC_Journal_Ed-23.pdf

Starling, C. and Mark Massa. “Russian nuclear anti-satellite weapons would require a firm US response, not hysteria.” *New Atlanticist*. 15 February 2024. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-nuclear-anti-satellite-weapons-would-require-a-firm-us-response-not-hysteria/#:~:text=It%20follows%20that%20an%20adversary,by%20destroying%20their%20own%20satellites.

Strout, Nathan. “NATO’s new tool shows the impact of GPS jammers.” *Defence News*. Updated 15 April 2020. https://www.defensenews.com/newsletters/military-space-report/2020/04/15/natos-new-tool-shows-the-impact-of-gps-jammers/

Thomas, Timothy L. “Russia’s Asymmetric Concept: Based on Military Art, Geopolitics, and Risk.” In Russian Military Thought: Concepts and Elements. McLean, VA: MITRE Corporation, (August 2019): p. 5-1 to 5-12

https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf

Xu, Shaoxing. “Electronic Warfare in China’s Past, Present, and Future”. Last modified 29 November 1995. https://apps.dtic.mil/sti/citations/ADA304506