National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

ELECTROMAGNETIC SPECTRUM CAPABLITY: CRITICAL TO THE FUTURE FIGHT

Major Richard Hough

JCSP 50

Service Paper

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

Étude militaire

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

Service Paper – Étude militaire

ELECTROMAGNETIC SPECTRUM CAPABLITY: CRITICAL TO THE FUTURE FIGHT

Major Richard Hough

ELECTROMAGNETIC SPECTRUM CAPABLITY:
CRITICAL TO THE FUTURE FIGHT

AIM

1. Electronic Warfare (EW) is a specialized branch of the military, which is often done below the threshold of public perception. Modern western military operations have become more reliant on the electromagnetic spectrum (EMS) for mission success due to the reliance on the Global Positioning Satellite System (GPS), radios and other computerized systems. While not making specific recommendations, this paper will highlight the threat posed to future operations should EMS equipment and training not receive increased awareness and funding priority from operational commanders.

INTRODUCTION

2. Recent Royal Canadian Air Force (RCAF) operations have occurred where there was either air superiority (e.g., Libya) or air supremacy (e.g., Afghanistan). Operations in these environments have allowed for relatively unopposed air operations, resulting in reduced consideration of enemy actions in the air planning cycle. For operations where the airspace was potentially contested (Syria), government direction precluded RCAF assets from being used where there was a significant threat to aircraft. While future conflicts may also occur in a permissive environment, it is prudent to assume that a more contested environment will be created by a peer/near peer adversary, or their proxy. One of the easiest methods to contest airspace is through the use of the EMS. Operations within the EMS are also refered to as electromagnetic spectrum operations (EMSO).

3. With a brief look at some potential future adversaries and their concept of EMSO, a case will be made for the requirement to increase RCAF capability to operate in a theatre where the adversary is employing EMS denial techniques. Discussion of some potential areas of vulnerability will be examined. A review Canada's EMS training and research capability will also be mentioned. Discussions in this paper will be done at the unclassified level. Should further information be required, the Senior Staff Officer for Electronic Warfare at 1 Canadian Air Division (SSO EW 1 CAD) should be engaged.

DISCUSSION

4. Military operations in the EMS are extensive. These can include the use of navigation devices such as GPS, radio communications, satellite communications (SATCOM) and aircraft protective systems. Each of these have the potential to be affected through adversary EMSO. While some devices are less susceptible to adversary interference (think low power communication systems or laser communications), there are operational tradeoffs to these technologies. A region with systems to prevent an attacker from bringing in their systems or preventing them from using these systems freely is commonly referred to as an anti-access / area denial (A2AD) region / area.[1] An A2AD area may be created through the use of electronic measures or through physical means such as the installation of air defence systems.[2]

[1] Andreas Schmidt. "Countering Anti-Access/Area Denial." *Transforming Joint Air Power: The Journal of the JAPCC.* No 23 (Autumn/Winter 2016): 70.

[2] *Ibid*. 72.

5. Based on the CDS statement that a focus is required on Russia and China as potential adversaries, their capabilities and intentions in the EM spectrum are applicable to this issue.[3]

6. Russia has been developing and fielding EW equipment which encompasses much of the EMS within the past 20 years.[4] According to open sources, these capabilities include the ability to jam radars, satellite communications, radio communications, GPS and drone control systems. Within the radio communications is the capability to affect high frequency (HF), very high frequency (VHF), ultra-high frequency (UHF) and cellular devices.[5]

7. The frequencies covered by the above systems involve much of the spectrum that the RCAF would intend to utilize in a future combat scenario against either Russia, or a Russian sponsored (and supplied) adversary. If employed by Russia, or Russian backed forces, these EMSO capabilities would impact Allied forces freedom of movement, targeting ability, command and control and increase the probability of excessive collateral damage. It should be anticipated that EW effects would be observed by Allied forces and these systems would have to be countered to achieve mission effects.

8. The Russian military have recognized EW as a force enhancer. "Russian EW troops are meant to disrupt the adversary's command control and communication systems and consequently to disorganize its forces and weapon systems."[6] Knowledge of EW and EMSO subsequently become essential to countering the Russian intent to utilize EW against our forces. Russia has used EW forces in Ukraine, and it is anticipated that they will continue to use them in future conflicts, including in areas outside of Russia proper, such as in Belarus.[7]

9. Similar to Russia, there is open source evidence for a Chinese EW capability. According to a document which was translated by the US Defense Technical Information Center (DTIC), the Chinese military leadership believe that "fighting for supremacy in the electromagnetic spectrum has become key to success or failure in war."[8] Much of the open-source documentation show that China has a focus on communications jamming, however, as described later, they also have a capability to affect navigation satellites.

10. In addition to the communications effects that Chinese EW capabilities may have, it is recently reported that they have fielded a system which is capable of following frequency agile radars and other electronic warfare pods which are employed on aircraft such as the F-15, F-16,

---

[3] Canada. Department of National Defence. "Pan-Domain Force Employment Concept: Prevailing in an Uncertain World." Ottawa: CJOC, 2023. 39.

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

[5] *Ibid.*

[6] Pavel Luzin. "Electronic Warfare: Russia's approach." *Foreign Policy Research Institute: Eurasia Program.* Februrary 2022. 16. https://www.fpri.org/wp-content/uploads/2022/02/electronic-warfare-022222.pdf

[7] *Ibid. 18.*

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

MiG-27 and MiG-29 fighters. While not confirmed, this should be viewed as a possible threat to aircraft self-protection jamming systems.[9]

11. GPS is a system which is integrated into many different RCAF assets, from aircraft to the weapons that are delivered. One reason for the use of GPS guidance with munitions is the assumption of reduced collateral damage due to the accuracy of these devices. Unfortunately, this is not guaranteed in an A2AD environment. As has been observed during the current conflict in Ukraine, Russia does not appear to have a similar concern for collateral damage as the Allied forces, and may not require the precision of GPS guidance for their weapons. During a conflict with a Chinese-sponsored attacker, it can be presumed that the Chinese navigation system (Beidou) could be their primary navigation system, making the US GPS system redundant and therefore a potential target.

12. Some regions and buildings in China are being intermittently protected by GPS jammers / spoofers according to recent reporting.[10] While the examples provided in much of the recent journalism focuses on the maritime threat, the use of GPS protection should be considered for weapon delivery, and potentially airborne navigation as well. One technique that has been utilized has all GPS signals spoofed from a target area to a single point, well away from the protected facility (Russian technique).[11] An obvious military application of this becomes protection of a high value target from GPS guided munitions. The spoofed location could be either a random location, or a point specifically chosen by the adversary to maximize damage to the alliance effort.[12] It is suspected that Russia has been using GPS spoofing and jamming techniques as one method of providing protection to VIPs within Russia.[13]

13. It should be assessed that any future adversary, if Russian or Chinese sponsored, will have the capability to affect RCAF and allied operations within the EMS. These effects will be noticed in communications, navigation and targeting aspects of the conflict.

14. The use of EW operationally does not need to be obvious to the target entity. It is feasible that the target of an EW attack is unaware that their systems are being affected until they have employed a weapon with no chance of recall, or provided targeting coordinates to others. The result is that all operators require sufficient training and understanding of adversary EW capabilities prior to deployment. This knowledge should include possible effective countermeasures and the protective measures included in their equipment.

---

[9] 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

[10] 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

[11] Mark Harris. "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/

[12] Eg. a precision guided weapon which hits a culturally protected facility. Adversary propaganda efforts could then portray ally efforts as illegal in the international order.

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

15. The later two items of training are provided at the fleet level (if provided), and should be included in regular training programs. The first training activity is provided at the basic level through two programs offered through Barker College in Winnipeg and one offered through the Royal Military College (RMC) in Kingston. The maximum student load for the most advanced course offered is 24 students yearly, with around six of those spots being reserved for 414 (EW) Sqn personnel. To prepare for a future A2AD environment, this throughput is not sufficient to maintain capability much less remove the current deficiency in training that currently exists.

16. The RCAF is in the process of on-boarding for the F35, which is an asset containing stealth properties. While this will assist in operations in an A2AD environment, applying stealth to air assets is not a solution to all the A2AD issues. This can be seen by the reporting on the F117 Nighthawk being shot down over Serbia by a Russian made SA-3 Goa (S-125)[14] In this case, the Serbian air defence personnel were able to provide area denial against a modern aircraft using a system originally designed and built in the late 1950's.[15] It can be anticipated that while aircraft stealth capabilities have improved, air defence capabilities against this type of protective measure will also have improved. It should not be assumed that stealth aircraft will be able to operate in an A2AD environment unopposed.

17. Stealth aircraft development dates back to the 1970's with a US Defense Advanced Research Projects Agency (DARPA) project which investigated technologies to reduce aircraft radar signatures. This was done through the development of radar absorbent materials (RAM) as well as shaping of the aircraft design and resulted in the F-117A stealth fighter.[16] The technology developed during this program has since evolved to include such aircraft as the B-2 bomber and the F-35 Lightning II fighter aircraft.

18. Shaping of an aircraft works in a similar concept to the use of mirrors, where the incoming radar beam is reflected away from the anticipated location of the receiving antenna. While this works well for many traditional transmitter/receiver pairs, it may not be effective to future bi-static systems where the receiver and transmitter are not co-located. Given that the shape of an aircraft is determined during the fabrication of this airframe, changing this countermeasure will take a prolonged time. As a result, aircraft may be vulnerable in an A2AD environment for the duration of a conflict.

19. RAM are a special coating which can be applied to aircraft structures which convert radar energy into a different form of energy, such as heat. Unfortunately, these materials only work for a few frequencies.[17] To get broad coverage across the EMS, a variety of different RAMs would

---

[14] Andrew Metrick. "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/

[15] Federation of American Scientists. "S-125 SA-3 GOA" updated 3 July 1998. https://nuke.fas.org/guide/russia/airdef/s-125.htm

[16] DARPA. "DARPA's Stealth Revolution." Accessed 18 February 2024. https://www.darpa.mil/about-us/timeline/darpas-stealth-revolution#:~:text=In%20the%20mid%2D1970s%2C%20DARPA,became%20operational%20in%20October%201983

[17] Kevin Gaylor. "Radar absorbing materials – mechanisms and materials." Accessed 18 February 2024. apps.dtic.mil/sti/tr/pdf/ada215068.pdf

need to be used. This would add weight to the aircraft design, potentially rendering a design ineffective. While these materials reduce the radar signature of an aircraft, they increase the signature in a different portion of the EMS, increasing the effectiveness of a different class of weapons. The adversary could also use multiple portions of the EMS in the radio wavelength and potentially still be able to track the aircraft due to damaged or missing RAM coverage of a particular frequency.

20. These technologies can still be vulnerable to anti-aircraft systems which are attempting to create the A2AD region. Given that the technology has been in the public domain for over 30 years, it should be assumed that any advanced adversary has developed countermeasures to be used against aircraft using stealth technologies alone. A combination of aircraft design, paired with active measures may provide better protection with the advantage of being able to modify active measures in a much more rapid fashion.

21. Canada has two main defence sponsored organizations which deal with EMSO in the academic / research regime. These are Defence Research and Development Canada (DRDC) Ottawa and Valcartier. The two organizations work in different portions of the EMS, and have developed spectrum specific expertise in their respective portion of the spectrum. DRDC (Ottawa) specializes in communications, radar, cyber and space, while Valcartier specializes in the optical portion of the spectrum.[18]

22. While most of their work is done directly in support of defence requirements, products which result from their research are not necessarily further developed into defence products. An example of this is when DRDC (Ottawa) developed a radio frequency jamming capability which was able to produce jamming waveforms which could counter adversary radar signals. This device remained a research tool for more than a decade and was never further developed into an operational capability. The device permitted DRDC (Ottawa) to determine techniques to protect RCAF aircraft should an operational capability be acquired. A follow-on project was also developed, with positive results, but there is no current plan to turn this research project into an operational capability.

CONCLUSION

23. To remain a credible threat in tomorrow's conflict, the RCAF needs to consider the future conflict environment. This means consideration of EMSO as it can be expected that our adversary (or their proxy) will use techniques to threaten / deny western militaries access to EMS technology / techniques. The permissive environment that the RCAF has become accustomed to during recent conflicts should not be expected in future conflicts.

24. Advancing the RCAF to an EMSO mindset will take time and resources. The time to develop a robust EMS program is not after a conflict has been started. Given that EMSO are classified, and may only become obvious once in direct conflict with a capable adversary, it is prudent to consider an adversary capable in these operations prior to any conflict. Producing

[18] Government of Canada. "Research and development capabilities." Last modified November 24 2023. https://www.canada.ca/en/defence-research-development/services/capabilities.html#toc5

effective counter techniques will continue to take a period of time, however, with sufficient investment in this type of operation will reduce the time required for the development of countermeasures.

25. Discussions in this paper have been at the unclassified level SSO EW 1 CAD should be engaged for a more in-depth analysis if desired.

RECOMMENDATIONS

26. Aircrew must include training in an A2AD environment in their regular training cycle. This can include simulator and live training activities where appropriate and where equipment permits. Acquisition of new EW training tools for operational squadrons, to include 414 (EW) Sqn, to allow for more realistic training scenarios should be considered.

27. Improve EW training for all RCAF personnel. Courses offered through RMC (Kingston) will help, however additional resources are required to increase student output.

28. Increased prioritization of EW equipment on Department of Air Requirements (DAR) acquisition lists. With long lead times on acquisition, modern EW systems need to be purchased quickly once the need has been identified.

29. Working with industry partners, operationalize EW research created by DRDC Ottawa and Valcartier. International partners may be interested in the end result, increasing Canada's reputation as a strong partner in the EW environment.

BIBLIOGRAPHY

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

DARPA. “DARPA’s Stealth Revolution.” Accessed 18 February 2024. https://www.darpa.mil/about-us/timeline/darpas-stealth-revolution

Federation of American Scientists. “S-125 SA-3 GOA” updated 3 July 1998. https://nuke.fas.org/guide/russia/airdef/s-125.htm

Canada. Department of National Defence. “Pan-Domain Force Employment Concept: Prevailing in an Uncertain World.” Ottawa: CJOC, 2023.

Government of Canada. “Research and development capabilities.” Last modified November 24 2023. https://www.canada.ca/en/defence-research-development/services/capabilities.html#toc5

Gaylor, Kevin. “Radar absorbing materials – mechanisms and materials.” Accessed 18 February 2024. apps.dtic.mil/sti/tr/pdf/ada215068.pdf

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

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/

Luzin, Pavel. “Electronic Warfare: Russia’s approach.” *Foreign Policy Research Institute: Eurasia Program.* Februrary 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/

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

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