National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

BREAKING THE KILL CHAIN: CANADIAN SPECIAL OPERATIONS FORCES AND ANTI-ACCESS AREA-DENIAL

Major Declan Ward

JCSP 47

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 47

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 47 - PCEMI 47
2020 - 2021

SERVICE PAPER – ÉTUDE MILITAIRE

BREAKING THE KILL CHAIN: CANSOF AND ANTI-ACCESS AREA-DENIAL

By Major Declan F. Ward

Word Count: 2,636

Nombre de mots : 2.636

BREAKING THE KILL CHAIN: CANSOF AND ANTI-ACCESS AREA-DENIAL

AIM

1. This service paper examines the role of Canadian Special Operations Forces (CANSOF) in countering near-peer adversary Anti-Access Area-Denial (A2AD) systems as a part of Great Power Competition (GPC). It is focused on providing analysis and viable recommendations to Canadian Special Operations Forces Command (CANSOFCOM) on where CANSOF can be best utilized in a Combined/Joint context. As an unclassified document, it will not discuss specific Tactics, Techniques, and Procedures (TTPs) nor will it identify capabilities in detail.

INTRODUCTION

2. Since its establishment in 2006 CANSOFCOM has been conducting continuous operations to directly and indirectly address the problem of Violent Extremist Organizations (VEOs). This focus on VEO's has resulted in a force that is optimized to carry out Counter-Terrorism (CT) and Counter-Insurgency (COIN) missions against non-state adversaries. While CANSOF have been successful in carrying out many such operations, it has meant that broader capabilities and competencies related to major combat operations against state actors are less developed. This poses a problem as the 2020 CAF *Pan-Domain Force Employment Concept* notes that "the magnitude of [the GPC] challenge is far greater than other threats, including that posed by [VEOs]."[1]

3. At the same time that CANSOF (and allied forces) were focused on COIN/CT, potential state adversaries developed a range of new military capabilities aimed at contesting western

[1] Canadian Armed Forces, *Pan-Domain Force Employment Concept, (*Ottawa: Department of National Defence, 2020), 12.

dominance.[2] The centrepiece of these new capabilities is the network of sensors and long-range fires that make up A2AD. A report commissioned for the US Congress describes A2AD in the following terms,

> Both China and Russia have fielded advanced warfighting capabilities to include mobile ballistic missiles, mobile air and coastal defense weapon systems, cyber, stealth aircraft, remotely piloted aircraft, advanced ISR [intelligence surveillance and reconnaissance] and electronic warfare capabilities; they are also pursuing emerging weapon systems and capabilities that may significantly impair the current U.S. ISR enterprise by forcibly denying platforms and sensors both geographic and virtual access to adversary activity and data. [3]

This layered approach of SENSE and ACT capabilities creates a bubble where conventional forces are unable to mass or indeed carry out their own SENSE and ACT functions. Some of these capabilities were demonstrated in 2014, when Russia annexed the Crimea from Ukraine and supported an ethnic Russian separatist government in the Donbas region.[4] While A2AD systems are being fielded by a number of potential adversaries, this discussion focuses on the Russian case as the CAF presently has elements deployed to deter Russian regional aggression under the rubric of Operations UNIFIER and REASSURANCE, and Russia has deployed A2AD systems that can reach into NATO's Eastern flank from Kaliningrad and Crimea.[5] The discussion below considers this region of NATO as the optimal space for CANSOF to counter A2AD, as opposed to consideration of deep strike options into Russian territory. CANSOF's unique ability to

[2] Brose, Christian. *The Kill Chain*. (New York, NY: Hachette Books, 2020), 26-31.

[3] Smagh, Nishawn. *Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition*. (Washington D.C.: Congressional Research Service, 2020), 7.

[4] *"Little Green Men": A Primer of Russian Unconventional Warfare, Ukraine 2013-2014*. (Fort Bragg, North Carolina: The United States Army Special Operations Command, 2015), 33; Brose, Christian. *The Kill Chain*…22.

[5] Schmidt, Andreas. "Countering Anti-Access/Area Denial - Future Capability Requirements in NATO." *The Journal of the Joint Air Power Competence Centre* 23, (2016), 71.

conduct *Special Warfare (SW)*[6] activities is ideally suited to counter peer adversaries' actions in potential conflict zones *before* an A2AD bubble becomes active.

DISCUSSION

The A2AD Problem

4. Countering A2AD is a significant undertaking given that the concept and systems it employs are purpose built to counter militaries like the CAF. However, A2AD systems are far from invulnerable, and many militaries, including the US and UK, are putting significant effort into addressing A2AD strategies.[7] At present Canada is working on delivering the capabilities outlined in *Strong, Secure, Engaged: Canada's Defence Policy (SSE),* which are focused on Grey Zone conflict.[8] A2AD is mentioned only once in the strategy and is linked to the replacement of the CF-18.[9] Given the scale of the A2AD challenge and the fact that "Canada does not operate alone," [10] it is unsurprising that Canada has chosen to invest in multi-purpose forces over developing exquisite capabilities to take on A2AD systems. However, the logic of this approach does not make the A2AD problem disappear, nor absolve the CAF of the requirement to address it. Fortunately, many of the approaches and competencies resident in CANSOF can be built upon to address the challenges of A2AD.

---

[6] SW is defined in US Doctrine as ""special operations forces conducting combinations of unconventional warfare, foreign internal defense, and/or counterinsurgency through and with indigenous forces or personnel." See: Headquarters, U.S. Department of the Army, *Special Operations*, Army Doctrine Publication 3-05, (Washington, D.C., August 2012), 9.

[7] *Integrated Operating Concept 2025*. (London: UK Ministry of Defence, 2020), 7; Mattis, James. *Summary of the 2018 National Defense Strategy of the United States of America*. U.S. Department of Defense. Washington, 2018, 6.

[8] SSE defines 'grey zone,' as an approach "that exists just below the threshold of armed conflict […]By staying in the fog of the grey zone, states can influence events in their favour without triggering outright armed conflict." See: Government of Canada, *Strong Secure Engaged*, (National Defence. Ottawa, 2017), 53.

[9] Ibid., 38.

[10] Rouleau, Michael, "*VCDS Keynote Address."*Network for Strategic Analysis, (10 December 2020).

5. A2AD is best understood as an asymmetric response to US/Western dominance in conventional military operations, showcased by the campaigns in the First Gulf War, the Kosovo Air Campaign, and the 2003 invasion of Iraq.[11] By denying western forces theatre approaches to mass or employ preparatory fires prior to operations, A2AD limits western crisis response options to nuclear response or conducting large-scale Joint Forcible Entry. These options represent the two most costly military responses available and are therefore unlikely to be employed apart from under the most extreme circumstances. This dilemma speaks to the strategic nature of the A2AD problem: it is a tool of GPC designed to impose unacceptably high costs on intervention. It is closely linked to another strategic approach: that of Grey Zone activities, which shape the environment pre-crisis, like in early 2014 when in a period of only weeks Russia was able to annex the Crimea from Ukraine without firing a shot.[12] Such strategies have worrisome implications for global stability as it leaves western countries with only bad options: let adversaries carry out actions against our interests, or intervene and escalate a conflict where victory is not assured and casualties could be massive. However, there is another option for the CAF and allied militaries: contest and mitigate A2AD systems and return conventional deterrence to the global strategic landscape through limited military intervention.

The SOF Approach and A2AD

6. As the fight against Daesh in Northern Iraq showed, small teams of CANSOF conducting SW can enable much larger local forces to address complex tactical and even operational problems, all while minimizing exposure of CAF personnel. In the context of A2AD, deploying CANSOF elements into vulnerable areas impacted by potential A2AD bubbles would achieve a

[11] Kilcullen, David, *The Dragons and the Snakes*, (Oxford: Oxford University Press, 2020), 29.
[12] *Little Green Men…57.*

number of positive outcomes. First, CANSOF's ability to train and mentor local allies will better prepare them to face both the Grey Zone activities of adversaries, and any potential escalations in the conflict. Having CANSOF teams forward deployed will also allow for the conduct of activities to understand the environment and prepare contingencies should the conflict escalate. Having a persistent CANSOF presence inside of the adversaries A2AD bubble can help address many of the challenges of penetrating the bubble from the outside, enabling either additional SOF or conventional forces to be brought into theatre.

7. Conducting SW activities under such circumstances would require the employment of SOF insertion methods and unique TTPs to offset the OPSEC and force protection concerns that would arise with conventional deployments, as it would be a near certainty that adversary militaries and national intelligence services will want to collect intelligence against CANSOF. Similarly, were the conflict to escalate, CANSOF's light footprint and capabilities to operate in sensitive/denied areas, coupled with its local networks, would reduce risk to force in comparison to other options. Given adversary access to resources and advanced capabilities CANSOF must constantly re-evaluate both TTPs and capabilities to ensure they continue to be fit for purpose and not compromised.

SOF as a Strategic Tool *BEFORE* a Crisis Occurs

8. From a strategic perspective, having CANSOF forward deployed sends both allies and adversaries a strong message about commitment. Putting any forces into a potential conflict region sends clear signals about deterrence; using SOF adds an additional layer as it provides ambiguity that can be indispensible if adversaries are able to mitigate joint conventional capabilities. Properly employed the presence of SOF can cause adversaries to revisit the strategic

calculus of certain actions, as they cannot be sure of what SOF is able to do or where they are located. More importantly, SOF acts as a sensor that can provide intelligence and early warning of adversary actions from *inside* of an area that is supposed to be denied to western forces. While SOF provides decision makers with timely and accurate information, it presents adversary decision makers with the dilemma of not knowing whether or not their A2AD system will be compromised, which raises the possibility of a western response and may in turn deter adversary action.

SOF in the Multi-Domain Fight

9. Should a conflict with a peer adversary escalate and A2AD systems go active, CANSOF elements would be able to provide a number of effects both through a SW approach, and unilaterally. While under ideal circumstances CANSOF would have a forward presence inside the bubble, given the focus of A2AD systems on conventional forces, CANSOF's unique capabilities to infiltrate into denied areas are ideally suited to penetrate the bubble. Once inside the conflict zone the role of CANSOF would need to be carefully considered, as such forces would be made up of small teams with limited or no access to external support (a situation which they are selected and trained for). While CANSOF could provide support to partner forces conducting large scale operations, it would be best employed leveraging its Special Reconnaissance (SR) and Direction Action (DA) capabilities to target key elements of the adversary's A2AD network and its kill chain.[13]

[13] In this context the kill chain refers to the process of sensors detecting targets in the environment and how that data is communicated to commanders who decide on what action to take, and to shooters who then prosecute the target with fires (both kinetic and non-kinetic).

10. Conducting SR and DA missions in an A2AD environment will require CANSOF to adjust capabilities that have been optimized for targeting VEOs. CANSOFCOM has broadly identified this requirement in its 2019 *Future Operating Concept Handbook*,[14] and careful consideration must be given to the development of such capabilities. Based on the available information about the 2014 Donbas Invasion in Eastern Ukraine, it is apparent that Russia in particular is heavily invested in SENSE capabilities in the electromagnetic (EM) spectrum and has developed a highly evolved kill chain of prolific UAS sensors linked to both Armed UAS and ground based fires.[15]

11. What this means for CANSOF is that individual SOF teams must be able to execute their own kill chain using only organic assets, as using communications to pass targeting data to external shooters would open teams to rapid geo-location and strike by enemy systems. Similarly, when engaging with organic fires, CANSOF elements will need to consider the responsiveness of the enemy kill chain. This likely precludes the use of most current CANSOF weapons, as they lack the standoff to safely engage the target without putting the shooter at risk. The ACT function in such an environment is best achieved through the use of standoff weapons like UAS and very long-range ground based fires like guided missiles, as well as electronic attack (EA) systems that can counter the sensors and shooters the enemy uses. Employed in conjunction with TTPs that emphasize stealth, such systems would permit CANSOF to degrade the enemy kill chain to the point that Joint Fires could then be called to further degrade the A2AD system. Once the A2AD bubble is sufficiently degraded, conventional forces could then be brought into the fight and leverage their advantages over enemy.

---

[14] CANSOFCOM. *Future Operating Environment Handbook*. (Ottawa: Minister of National Defence, 2017), 3.

[15] Brose, Christian. *The Kill Chain*…23.

12. This approach would require the employment of systems that are not currently in the CAF inventory. However, these very systems were used to great effect by Azerbaijan in the recent Nagorno-Karabakh conflict with Armenia. In this instance Azerbaijani forces used a combination of UAS, loitering munitions, and conventional ground fires to achieve decidedly one-sided results against Armenian forces.[16] The fact that a country of relatively modest means was able to field such a sophisticated and lethal set of capabilities should act as both a warning and an example for the CAF. Many of these systems are in the form of smaller UAS and loitering munitions with impressive standoff capabilities, while also being compact enough for use by small teams.

CONCLUSION

13. Although CANSOF has historically focused on counter-VEO operations, serious consideration must be given to transitioning a least a portion of CANSOFCOM's focus to the A2AD problem-set. Furthermore, the link between Grey Zone activities and A2AD must be explored in further detail. While this paper was focused on the latter; the two approaches are closely linked and should not be treated as discrete concepts. Many of CANSOFCOM's current strengths in the field of SW, SR, and DA can be shifted to addressing peer-adversary systems with a relatively modest investment in capability. In most instances the roles and capabilities required for counter-A2AD have application in any peer conflict setting. As the performance of the Azerbaijani military in fall of 2020 showed, investment in small-scale precision weapons and sensors can provide outsized effects against adversaries. With the appropriate authorities and

[16] Watling, Jack, "The Key to Armenia's Tank Losses: The Sensors, Not the Shooters," *RUSI Defence Systems* 22, no. 1 (6 October, 2020).

equipment CANSOF would be able to degrade an adversary's A2AD kill chain and enable the theatre entry of conventional forces able to dominate the battle-space.

RECOMMENDATIONS

Force Employment

14. CANSOCOM should forward deploy a Special Operations Planning and Liaison Elements (SOPLE) or a Special Operations Task Force (SOTF) to Eastern Europe as forward staging to counter-A2AD systems. The SOPLE/SOTF should act as a persistent presence to provide a SENSE function as well as facilitate episodic engagements by CANSOF teams conducting SW and Operational Preparation of the Environment activities. This forward deployed element must have the necessary authorities for broad intelligence collection and making preparations for an escalation in the conflict.

Force Generation

15. In the event of A2AD systems going active during a conflict CANSOF elements must be capable of synchronizing their actions within the wider Joint Force. To achieve this CANSOF must begin participating in Joint Force training with the CAF and Allies. A good start point for this is participating in the U.S. Joint Warfighter Assessment Series of exercises.

16. CANSOFCOM Force Generation should be adjusted to develop skills for activities in Grey Zone and A2AD settings. Specifically, this means Individual and collective training that trains operators and SOF teams to mitigate Counter-Intelligence threats and to avoid detection by sophisticated EM and other sensors. This would be best achieved by assigning a unit with the

task to develop TTPs and consider the Force Development requirements of operating in an A2AD environment.

Force Development

17. CANSOFCOM should acquire SOF team level capabilities for operating in an A2AD setting. All such systems must be able to be transported and powered by CANSOF mobility platforms. Furthermore, consideration must be given to ensuring such systems are low probability detect/intercept either though technical means or TTPs. Specifically CANSOF will require the following:

a. EM sensors and Electronic Attack equipment to locate and attack enemy sensors;
b. C-UAS systems;
c. long range[17] UAS as a sense capability;
d. loitering munitions and ground based precision fires with variable fusing and payload options, to include anti-radiation capabilities.

18. In addition to capabilities listed above, CANSOFCOM should invest in research and development of additional capabilities to ensure better force protection and interoperability with allies, including:

a. Medical capabilities for use inside the A2AD bubble as MEDEVAC timelines to move casualties to a secure facility will be extended.
b. High bandwidth, low probability intercept/detect operational and strategic communications links to pass target data outside the A2AD bubble.

[17] In this instance 'long range' denotes systems that can operate at ranges between 50-200km.

c. Low probability detect/intercept tactical communications for use by SOF teams inside the A2AD bubble.

d. The ability for CANSOCOM's tactical/operational data networks operate as part of a federated allied network.

BIBLIOGRAPHY

Brose, Christian. *The Kill Chain*. New York, NY: Hachette Books, 2020.

Canadian Armed Forces. *Pan-Domain Force Employment Concept* . Ottawa: Department of National Defence, Canada, 2020.

Government of Canada. *Strong Secure Engaged* .National Defence. Ottawa, 2017.

Headquarters, U.S. Department of the Army, *Special Operations*, Army Doctrine Publication 3-05, Washington, D.C., August 2012.

Integrated Operating Concept 2025. London: UK Ministry of Defence, 2020.

Kilcullen, David. *The Dragons and the Snakes*. Oxford: Oxford University Press, 2020.

"Little Green Men": A Primer of Russian Unconventional Warfare, Ukraine 2013-2014. Fort Bragg, North Carolina: The United States Army Special Operations Command, 2015.

Mattis, James. *Summary of the 2018 National Defense Strategy of the United States of America*. U.S. Department of Defense. Washington, 2018.

Strong Secure Engaged National Defence, 2017.

Rouleau, Michael. "VCDS Keynote Address."Network for Strategic Analysis, 10 December 2020.

Schmidt, Andreas. "Countering Anti-Access/Area Denial - Future Capability Requirements in NATO." *The Journal of the Joint Air Power Competence Centre* 23, (2016): 69-77.

Smagh, Nishawn. *Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition*. Washington D.C.: Congressional Research Service, 2020.

Watling, Jack. "The Key to Armenia's Tank Losses: The Sensors, Not the Shooters." *RUSI Defence Systems* 22, no. 1 (6 October, 2020). https://rusi.org/publication/rusi-defence-systems/key-armenia-tank-losses-sensors-not-shooters.