sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXVI No 1 2020

THE A2/AD CONCEPT IN THE FIFTH OPERATIONAL DOMAIN

George-Daniel BOBRIC

"Carol I" National Defense University, Bucharest, Romania
dbobric08@gmail.com

Abstract: *In the last decade, the world has faced a major change of the security balance, new directions of action being drawn by the main actors of the global scene. States are trying to expand their spheres of influence, to invest in research and technological development, especially to achieve the military superiority in different operational domains, to train their armies following the evolution of the security environment and the changing trends of conducting the armed struggle and to improve their military capabilities to gain or to maintain control over certain areas of interest. This is why, in the last years, the states have invested in military assets that can assure a complete implementation of the anti-access/area denial concept. Starting from the ideas that the A2/AD concept can be applied to all operational environments and that the cyberspace is the fifth domain of the armed struggle, in this paper, after a short glance at the increased interest of three powerful countries in this particular concept, a fastidious excogitation on it will be performed in the second part, while the third part will contain information regarding the cyber operations and their role in implementing the A2/AD concept in the battlefield characterized by 0s and 1s and, lastly, the main objectives of pursuing cyber attacks will be analyzed.*

Keywords: A2/AD, security, cyberspace, cyber attack

1. Introduction

The international geopolitical configuration faces today a shift from a unipolar to a bipolar or, according to other authors, multipolar world, where the main actors compete to achieve a common desideratum: the hegemony against other states on multiple domains, the military one having a special role through the well-known "arms race". The military operations have been performed, for several centuries, in three operational domains: land, sea and air. In the last decades, two more domains have become subjects of analyses, discussions and debates: space and cyberspace [1].

Nowadays the cyber domain's evolution is more and more self-evident. The use of cyber technology in day by day activities is a reality that cannot be contested. Also, the cyber domain is ubiquitous in the military operations, especially in those performed by the high-technologized actors. Latterly, a sort of "arms race" has been increasingly occurring when referring to the means and methods used by the cyber actors to reach their political or military goals. On the other hand, even if the cyber war has its beginnings more than three decades ago, cyber attacks became the new dimension of the strategic competition between the world's main actors. Also, in the specialty literature, an important role is held by the A2/AD concept and the methods of implementing it in analyzing, planning, coordinating and executing the military actions.

The A2/AD concept can be seen as having a special role at the three most important actors of the geopolitical scene: the U.S.A., Russia and China. In the United States, this

DOI: 10.2478/kbo-2020-0003

concept was fastidiously analyzed in 2003, as the main factor that could interfere with the United States armed force's ability to conduct, sustain and execute power-projection operations [2]. Secondly, the People's Liberation Army's point of view regarding the operations which can generate the anti-access/area denial effects mainly consists of non-kinetic technology development, submarines and missiles. The strategy of the Chinese army is to avoid contact battles and to strike against the adversary's unknown weaknesses. Such feebleness is provided, in the majority of cases, by the cyber domain. As a result, China's military analysts believe that the strongest point of America's military superiority is the C4I (command, control, communication, computer, intelligence) networks, thus seeking ways to disrupt them by targeting these facilities with cyber attacks [3].

The anti-access/area denial operations also have a special role in the Russian Armed Forces. As it can be seen, the Russian A2/AD systems are located in areas where the Russian Federation has strategic interests: Kaliningrad - for the Baltic Sea, the Crimean Peninsula - for the Black Sea, and Syria, where Russian systems created an umbrella to protect themselves and their Syrian allies against the Turkish military aviation and/or navy. The Russian A2/AD systems consist of a long-range of military high-tech equipment, like anti-ship, anti-air and anti-land systems assets. When it comes for the A2/AD concept implemented within the Black Sea area, there can be found the following important assets [4]: Bal and Bastion coastal defense systems, S-400 air defense system, defended by the Pantsyr-S1 anti-aircraft missile and gun systems, three frigates and six submarines with the Kalibr cruise missiles aboard, radar systems, etc.

Cyber domain has recently become a new battlefield, and the cyber operations have been conducted either concomitant or consecutive, to defeat the enemy's will of fighting. As any operations performed in the air, sea or land domains, the cyber operations can also be used to implement the strategic concept of anti-access/area denial. In this paper, the linchpin will be the fastidious analysis of the cyber domain in accordance with the role that it has in implementing the anti-access/area denial concept within the military operations.

2. The A2/AD concept

The anti-access/area denial concept is not a new notion. History shows that states implemented all sorts of strategies in order to block the enemy's entrance within a certain area of interest or to diminish its freedom of movement if it had managed to enter into a specific zone. A great example of area denial dated centuries ago is the strategic construction of the Great Wall of China, built in order to protect the Chinese empire against the various enemies. Also, closer to these days and in our vicinity, the Turks managed to implement the anti-access notion against the Anglo-French enemy in the First World War by closing the Dardanelles Strait, thus leading to a victory for the Turkish army. In the Cold War period, the technological innovations within the military domain conducted to an extent of range and lethality of the means of war-fighting and, finally, to an increased capability to implement the military will into a certain area of interest.

As for the NATO countries, this concept entered in the vernacular in the past years, especially after Russia's seizure of the Crimean Peninsula. The development of the armed forces of the Russian Federation, both in the training and in the military assets, in the last years, shows a trend of improving the capabilities of blocking an enemy from entering and acting in a specific area or neutralizing it in case it managed to enter in their area of strategic interest. But for NATO, the implementation of the A2/AD concept is problematic from three points of view. First of all, NATO had to shift its strategic role from assurance, up

to 2014 and, since then, to deterrence. In order to apply the new concept, the Alliance had to create the Very High Readiness Joint Task Force but, in reality, the main problem is that the Alliance has a drawback resulted from the scarcity of forces, on one hand, and from the variable level of interoperability between all the nations' equipment, personnel, techniques and procedures. Secondly, the power of some member countries to conduct military operations in a non-permissive environment is at a low stage. Lastly, a conundrum in the political and military domains is present: if the A2/AD is considered to be a defensive concept and NATO is a defensive alliance, why will not the member countries develop assets that will permit the entire agnation to reach the necessary combat preparedness and technical endowment for the adequate implementation of the above-mentioned concept?

This wide-used notion is composed of two key elements that are hard to be delimited. Firstly, the anti-access refers to the use of means and methods, by an actor, in order to limit the ability of its enemy to enter into a specific area of operations and to execute naval or aerial power projection. Secondly, considering that the anti-access actions did not manage to stop the enemy from entering in its own area of responsibility, the area denial operations aim at minimizing the freedom of movement/manoeuver in the area it entered and at stopping it from advancing in the zone. Also, as these can be applied to the physical layer of the armed struggle, another operational domain is worth to be analyzed from this conceptual perspective: the cyberspace.

3. A2/AD operations in the cyber grids

Cyber operations are different from those conducted in air, land or water, due to the fact that there is no need for a military conflict in order to be performed, but these can also be executed in peacetime.

In the cyberspace, A2/AD operations can be conducted on two operational levels: tactical and strategic. At the tactical level, cyber anti-access/area denial operations aim at deterring an enemy from entering into a specific zone or reducing its capability to accomplish the mission given, by targeting specific equipment. For example, an enemy cannot operate effectively if the GPS is not working at all or if the data displayed on the screen were corrupted and modified by a hacker. But at the strategic level, cyber operations are not conducted in order to deny the targeted state's ability to effectively use an asset, but to affect its ability to plan, develop, conduct and execute operations in the physical domain (as an example, the adversary could execute a preemptive cyber strike against its enemy's C4ISR – command, control, communications, intelligence, surveillance and reconnaissance - network, in order to completely "blind" it) or to fully block its access at the cyber grid.

At the tactical level, cyber operations are mainly executed to lead to kinetic effects. One can hack the soldiers' mobile phones in order to impersonate them and gain information relevant to the cause. As an example, a hacking group called Fancy Bear, believed to be affiliated to the Russian foreign intelligence agency (GRU), managed to create an application that was used against the Ukrainian soldiers. Through this malware, Russian hackers were able to reach the following goals [5]:

- to identify the chain of command of the military personnel on the battlefield, by reading the messages sent from the impersonated mobile phones;
- to determine the future operations plan;
- to locate the disposal area of the military units;
- to determine the soldiers to defect, by sending messages to their phones and by asking them to save their lives or even by convincing a member of the soldier's family to intervene and to demand him to withdraw from the army.

These actions mentioned above converge to a series of effects on the battlefield, from

which two kinetic ones are worth to be presented. Firstly, the Russian army managed to conduct effective preemptive strikes against the Ukrainian artillery units, thus leading to the latter being unable to complete the mission they were assigned to. Secondly, the use of cyber attacks, in this specific case, shows a strong connection between the cyber operations and the psychological ones, the soldiers being unable to accomplish their mission due to the psychological loop they were driven into. In conclusion, cyber operations executed at the tactical level can lead to both kinetic and psycho-moral effects and can prevent an enemy from conducting effective actions in a specific area of interest.

On the other hand, cyber operations performed in the cyberspace at the strategic level are aimed at realizing tremendous, unthinkable effects, in order to entail the hinder of target's access at the cyber grid or to cumber its ability to use the means and methods of acting in the cyber domain. In the last decade, states and non-states actors realized the whopping advantages of using the cyber environment to achieve their personal goals, regardless of their nature (political, economic, etc.). In this sense, in the past years, the world has faced a series of cyber-attacks, whose origin has or has not been established until now, that managed to disconnect a country from the cyber networks. One of the most notorious examples is the case of North Korea being disconnected, for several days, in December 2014, from the Internet, after a large-scale Distributed Denial of Service attack campaign, which is believed to have been conducted by the United States in response to the cyber attacks executed by North Korean hackers (supposedly) against the Sony Pictures Entertainment company at the end of November 2014 [6]. Moreover, there are other two well-known cases of countries "disconnected" from the Internet: Egypt - on January 2011 and Syria - on November 2012.

As a result of these actions, states began to understand how vulnerable their grids are against cyber anti-access operations and pursued to find solutions to counteract these actions. For example, at the end of December 2019, Russian authorities announced that the country had been disconnected from the Internet and that the traffic had been routed to the internal network known as RuNet [7]. This action can be seen as an attempt to assure a back-up plan if the nation is subject to a cyber attacks campaign.

In the battlefield determined by 0s and 1s, strategic area-denial can be seen as the operations which cause specific effects that may conduct to misbehavior of the critical infrastructure elements of the targeted group or state, especially those that are considered to be assets of strategic importance. Also, area-denial in the cyber domain can be considered as the online offensive campaign planned and performed with the purpose, among others, of gaining a competitive advantage against the target or of disrupting its ability to conduct effective cyber operations.

4. Objectives subsumed to cyber A2/AD operations

At the tactical level, the scopes are quite obvious consisting, mainly, of achieving the goal of deterring the enemy through a series of kinetic effects. In this sense, the tactical A2/AD operations performed in the cyber domain are linked with the results expected in other operational domains: land, air, sea and space. But then, at the strategic level, things are more complicated and the results expected have a higher level of impact, experts [8] presenting four main objectives which can be also available in the cyber context:

1. *operational exclusion* - NATO's military power is hard to compete against. So, a NATO's adversary could seek to "draw the guidelines" of a future possible confrontation. In this sense, one could seek to sneakily introduce "cyber Trojan horses"

in the NATO member states' grids in order to gain the advantage at the desired momentum.

2. *operational degradation* - a vast number of NATO member states have advanced cyber capabilities and knowledge in this special domain, but there are still countries that have shortcomings in this field (capabilities, specialists, knowledge, procedures). Adding the important vulnerabilities of the commercial cyberspace, developing countries in the cyber domain are vulnerable to mass attacks against the cyber connected facilities, thus leading to a major security breach for the country in particular, and for the entire alliance, generally.

3. *strategic preclusion* - NATO is seen as the most important political and military alliance around the globe, created in order to cooperate on issues related to security and defense aspects and to solve crises wherever and whenever it is needed. A NATO's adversary could seek the opportunity to erode the trust that the states have on the alliance's ability to defend them, even against a cyber campaign. To do so, the enemy could create an environment of insecurity in which it could develop cyber means and methods in order to create A2/AD bubbles inside the agnation, thus leading to a decay of the alliance's internal power and trust.

4. *strategic exhaustion* - anti-access/area denial operations conducted at the strategic level in the cyberspace leads to an almost irreversible exhaustion of the adversary's power and will to engage in an armed struggle. Cyber attacks are characterized, in the majority of cases, by a disproportion between the source of the attack (small number of personnel, little money involved, no need for advanced technology) and the damage done to the target (from the financial perspective up to geopolitical aspects) [9]. In this case, an actor which would be targeted by an increased number of cyber attacks may feel unwilling to engage in a conflict due to its impossibility to handle the continually eroding effects.

5. Conclusions

Nowadays, a special role in military operations is granted to the cyber domain. Military analysts realized the opportunities offered by the cyber operations and the characteristics that make them special, compared to the actions performed in the physical space. The trends in this operational, virtual space show an increasing trend in the number of cyber actions performed against other countries by the high-technologized states.

On the other hand, anti-access/area denial operations have recently been considered by the military thinkers the linchpin of the armed struggle due to their potential to determine egregious backlashes and kinetic effects. These two above excogitated ideas interconnected led to the conclusion that, given the specificity of the cyber domain, the A2/AD operations performed inside the cyber grid, regardless they are performed at the tactical or at the strategic level, have the potential to overthrow the combat situation at any time and to lead from operational exclusion up to strategic exclusion, even for the most developed countries or for the strongest military alliances.

References

[1] Bobric G., *Proliferation of the means and methods in the fifth operational domain*, in the 25th Student's International Conference SECOSAFT, Sibiu, 2020.

[2] Krepinevich, A.F., Watts, B., *Meeting the Anti-Access and Area-Denial Challenge*, 2003, online at: https://csbaonline.org/research/publications/a2ad-anti-access-area-denial

[3] Cliff, R., et all, *Entering the Dragon's Lair. Chinese Antiaccess Strategies and Their Implications for the United States*, Library of Congress Cataloging-in-Publication Data, 2007, p. 23.

[4] Smura, T., *Russian Anti-Access Area Denial (A2/AD) capabilities - implications for NATO,* 2016, online at: https://pulaski.pl/en/russian-anti-access-area-denial-a2ad-capabilities-implications-for-nato/
[5] ***, *Use of Fancy Bear Android malware in tracking of ukrainian field artillery units*, 2016, online at: https://www.crowdstrike.com/resources/reports/idc-vendor-profile-crowdstrike-2/
[6] Delerue, F., *Cyber Operations and International Law*, Cambridge University Press, Cambridge, 2020, p. 489.
[7] Cîmpanu, C., *Russia successfully disconnected from the internet*, 2019, online at: https://www.zdnet.com/article/russia-successfully-disconnected-from-the-internet/
[8] Alcazar, V., *Crisis Management and the Anti-Access/Area Denial Problem*, in Strategic Studies Quaterly, Vol. 6, No. 4, Air University Press, 2012, pp. 50-52.
[9] Dinicu, A., *Cyber threats to national security. Specific features and actors involved*, in the Scientific Bulletin of the "Nicolae Bălcescu" Land Forces Academy, No. 38, "Nicolae Bălcescu" Land Forces Academy Press, Sibiu, 2014, p. 111.