No.1/2023, JANUARY-MARCH
https://doi.org/10.53477/2284-9378-23-07

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

Cyber and space domains – Impact on the development of the multi-domain operations

Commander Alexandru CUCINSCHI, Ph.D. Candidate*

*"Carol I" National Defence University
e-mail: cucinschi.alexandru@gmail.com

Abstract

The recognition of two new operational environments/domains, the cyber environment and the space environment, has led to the imagining of several "asymmetric" possibilities of engaging an adversary, with the aim of creating multiple dilemmas for the adversary, which it must take into account. This approach to military operations is currently associated with the new concept of multi-domain operations. However, it should be noted that not only the recognition of the two new environments, in addition to the three classic environments, constitutes multi-domain operations, but also the future operating environment as a whole is a triggering factor. Thus, in this article, my aim is to identify the extent to which the two new operational environments contribute to the development of the new multi-domain operations concept, with the aim of highlighting possible ways forward in terms of implementing the multi-domain operation concept and developing specific actions in and from the cyber and space environments. Following the analysis carried out, it was noticed that the cyber and space domains are gradually losing relevance within the phases of the multi-domain operation, while the actions are being fragmented and decentralized. This fact must be taken into account in the development of multi-domain formations.

Keywords:
security environment; multi-domain operation; cyber domain; space domain.

Although the cyber and space domains are generally seen as environments that enhance or support actions in the air, on land, and at sea, I believe that, in the current security environment, their relevance is no less important than that of the conventional domains. This is primarily due to the fact that they can affect the combat power of a potential adversary or own forces to such an extent that the percentage of forces affected by them can be decisive in the outcome of a conflict, even before a conflict reaches the stage of open conflict.

I believe that this is, in fact, the typology of the new type of conflict, in the sense of the achievement of objectives by means that do not exceed the limit considered to be a trigger for the planning and conduct of conventional military action, such as the initiation of a conventional war. Thus, the two new domains seem to lend themselves to a large extent to what is circulating in the present and future security environment. This is also the reason why I consider that an analysis of the developments in the cyber and space environments is relevant nowadays.

However, we must admit from the very beginning that these environments influence, in the previously stated idea of fulfilling objectives without triggering an open conflict, a greater extent of the state's instruments of power other than the military, such as diplomatic, informational, and economic instruments. The military instrument of power is influenced to a greater extent only during the time frame in which the open conflict is triggered.

We observe a lack of linearity, in the sense that two domains attached to the classical domains and subordinate to the military instrument of power have a direct influence on the diplomatic, informational, and economic instruments of power, serving less the military instrument of power in what the multi-domain operations catalog as the competition phase. This complexity can be difficult to manage. However, it is necessary to analyze the elements that the two new environments introduce in their relationship with the classical environments and within the military instrument of power as a whole. This can lead to an awareness of the possibilities for the innovative use of armed forces in military operations.

Starting from the premise that the cyber and space domains aim, within military actions, to enhance and support actions from other environments (they can be categorized as force multipliers), I propose verifying the following research hypothesis: cyber and space domains will lead to the deduction of new tactics for the services operating in classic environments (including their innovative combination by the operational level) and will influence the way of achieving strategic military objectives. To draw pragmatic conclusions that confirm or refute the established research hypothesis, I will highlight the correlations established between the two new domains and the multi-domain operations as a whole, considering the data supposed to be used in this work.

The limitations of the research I am conducting, considering the fact that I am referring to a concept currently under development (multi-domain operations), are as follows:

- The multi-domain operations concept is not yet fully validated through war games and simulations, after which it can be refined;
- The interpretation of the relationships between the elements under study should be done from the perspective of the author's experience, given the novelty of the subject and the insufficient studies in this field.

The article is structured in three parts. In the first part, I will identify the elements considered defining for the two environments (cyber and space). Then, I will summarize the relevant aspects of multi-domain operations. In the last part, I will identify the correlations established between the two new environments and multi-domain operations.

1. Cyber and space domains – evolution and constituent elements

Elements from the cyber and space domains have been used since the 1950s, as follows:

- Computer tools were developed to store and process information, which could be used for offensive purposes but also needed protection.
- The first artificial satellite, Sputnik 1, was launched (International Institute for Strategic Studies 2015).

These developments have led to the identification of new options for engaging adversaries, generated by the emergence of innovative technologies that continue to develop today. However, since the end of the Cold War, military applications of these technologies have ceased to represent a priority due to the relaxation of the geostrategic situation. The interdependence and association between the two domains have been observed since the appearance of their basic elements. Currently, it is impossible to dissociate the cyber and space domains, and actions from one environment cannot be carried out without potentiation from the other environment.

Through longitudinal analysis, it can be observed that the cyber domain has undergone a more accelerated evolution than the space domain, most likely due to its accessibility for a diverse range of international actors through the advent of the Internet. However, this trend does not guarantee that the two domains will develop at the same pace in the future, and it is possible that opportunities identified in the cyber field will be exhausted while those in the space field represent greater interest for the development of new technologies and doctrines.

Next, in order to analyze how the two environments impact multi-domain operations and the military instrument as a whole, I will identify the essential elements of each environment as they are currently perceived.

1.1 Cyber domain

Although cyber actions, both offensive and defensive, have their origins in the 1950s with the emergence of information systems, their official recognition at the NATO level did not occur until 2016. At that time, the cyber domain was defined as an operational domain that must be defended as effectively as the air, land, and sea domains (NATO 2016). However, all actions in the cyber environment, as presented in the aforementioned document, are stated to be defensive in nature.

It is widely recognized that the majority of activity in the cyber domain (approximately 90%) is carried out in the private sector (Crowther 2017). This fact highlights the difficulties that the military faces in managing actions in and from this environment, given the multiple possibilities for action by various actors who are not bound by generally accepted rules. This contrasts with the clear rules that govern military operations.

While the military does operate in the cyber domain, their missions within this domain are not clearly defined. The actions that the military can perform or must be able to defend against are difficult to summarize under a certain classification. An approach to this issue, which I consider comprehensive and pragmatic, based on reference documents of the US and NATO that regulate general policies in this environment, was carried out by Dr. Glenn Alexander Crowther, a researcher in the field of cyber policies at the Institute National Center for Strategic Studies at the US National Defense University. It groups all of the military's actions with cyber implications into four categories centered around a set of common cyber actions (information and communications technologies, network operations, and defensive cyber operations) that represent baseline conditions for the identified categories.

The four categories identified in the mentioned study (Crowther 2017, 63-78) are, in fact, the implications of the cyber domain within the possible mission areas of the military, namely:

- Cyber information operations – within the missions in the information field;
- Cyber operations – within the framework of conventional and special operations carried out by the Armed Forces;
- Cybercrime – within missions that aim to reduce crime (the defence system usually has under it units that have such missions);
- Intelligence through cyber actions – within actions of interpretation/processing of information.

Examples in support of the identified categories are presented in the aforementioned work, but the extent to which these categories lend themselves to use in smaller militaries than the US is, in my opinion, difficult to quantify. Thus, I believe that with regard to developments in the cyber domain, it can be stated that the protection, manipulation, evasion, and use of information, aspects that summarize the categories presented, represent a sophistication of the basic mission identified since the emergence of this space in the 50s, that of information management.

As a result, although this elaboration of the core mission is not without foundation, given that technological developments have provided an increasingly wide range for the identification and innovative use of the tools that this environment can provide, I believe that it is important to remember that it is the information itself that directs developments in this environment.

1.2 Space domain

As in the case of the cyber domain, the space domain, although it has its origins in 1957, with the launch of the first satellite, Sputnik, by the USSR, it was designated by NATO as the fifth operating environment in December 2019, at the meeting of the leaders NATO member states (NATO 2022), thus recognizing the importance of this domain in issues related to the security of the Alliance.

The main threats that NATO has identified in this environment are related to physical effects in outer space and actions directed at capabilities in space:

- space is becoming an increasingly crowded and competitive environment, satellites being vulnerable due to interference;
- some states, including Russia and China have developed a wide range of anti-space technologies – NATO condemned Russia's testing of anti-satellite missiles on November 15, 2021 (NATO 2022).

Yet, I think it is much more important to highlight, from a military point of view, the fact that from this domain actions in all other domains can be influenced, so as a result, space is seen more as a potentate factor for actions in the other domains, without which the actions of the armed forces may be deprived of the advantage of complete information about a potential adversary. In this sense, the main concerns are represented by:

- the fact it represents an integrative environment for communications;
- it enables gathering, interpreting information in support of operations and missions;
- with the help of satellites, crises can be monitored and NATO can intervene effectively and in a timely manner (NATO 2022).

Thus, I consider that actions in the space domain can be divided into physical actions that take place in space on spatial means and actions that are directed towards the other four domains. The latter directly influence the activity of the military. However, it is evident that the development of capabilities to destroy satellites launched in this environment is envisaged to prevent the second category of missions in this environment. NATO divides space actions into actions to, from, and in space. "NATO has recognized that attacks to, from, or in space represent a clear challenge to the security of the Alliance and could lead to the invocation of Article 5 of the North Atlantic Treaty" (NATO 2022).

Regarding the solutions identified for gaining an advantage over a potential adversary in this domain, the actions identified as needing to be undertaken are represented by the ability of a space system architecture to provide persistent support for mission success despite hostile actions (Comparinni 2022). These include deterring the enemy from detecting and targeting space services or capabilities, ensuring reconstitution capabilities by launching new capabilities or activating reserve capabilities in orbit or on the ground, and supporting technologies such as quantum communications, continuous surveillance, advanced information algorithms based on artificial intelligence, and space robotics (Comparinni 2022).

It can be observed that the financial effort required to implement such solutions can be considered sustainable only by states or international organizations with a developed economic level and that possess advanced technologies or ongoing projects in this regard. Thus, I consider that in the case of the space domain, as with the cyber domain, information (obtaining, using, and prohibiting the use of information to the adversary) is what triggers the development of capabilities that will likely be directed to physical actions (such as jamming or attack) against the adversary's capabilities in the near future.

From what has been presented regarding the two domains, it can be stated that we are currently witnessing a "modernization" of the military instrument with regard to managing information through the use of innovative technologies, and that information itself can become a state policy. The two new domains, although not comprehensively controlled by the military, can decide the fate of a conflict from the early stages through specific actions in or towards them, just as a degree of airspace control greatly facilitates the success of operations in maritime and land environments. To verify the research hypothesis stated at the beginning of the article, the concept of multi-domain operation will be briefly described to subsequently determine the extent to which the two new domains contribute to the development of this concept.

2. Relevant aspects of multi-domain operation

The multi-domain operation is currently in the concept development stage, with an implementation horizon of 2028 for the USA (TRADOC 2018) and 2032 for the Romanian Armed Forces (presidency.ro 2020). This stage involves conducting war games to test the principles of this new type of operation, studying how to implement it, and refining the concept before starting the process of developing the necessary capabilities for implementation.

The development of this concept is necessary due to technological advancements that have made some aspects of classic joint operations impossible to implement. This is due to the increased precision and range of weapon systems, which have resulted in larger restricted areas (A2/AD) that prevent the support relation between services. Multi-domain operations aim to achieve favorable conditions for military actions and deter adversaries from triggering an open conflict. These aspects are included in the first phase of the operation (competition) and are dependent on the management of information in the two new domains. This can be seen in Table 1.

Thus, based on the defining elements of multi-domain operations presented in the TRADOC document, the concept can be divided into three main elements that contribute to understanding the new concept:

- information management (especially in the first and fifth phases – competition and return to competition in favorable terms) – actions that do not depend solely on the military instrument;
- addressing the A2/AD issue (phases two and three – penetration and disintegration);
- conducting joint operations adapted to the new conditions in the operational environment, through support between services (exploitation).

In the following section, I will explore the relationship between the main elements of the cyber and space environments and the defining elements of the multi-domain operation, as the integration of these new domains is important to gain strategic depth.

3. Relationships between cyber and space domains, multi-domain operation and strategic objectives

As the elements related to the two new domains as well as the summary description of the multi-domain operations were presented in the first two parts, I will briefly present some aspects related to the strategic depth, considering the fact that, mainly, the purpose of an operation, in our case multi-domain operations, is to contribute to the achievement of strategic level objectives. However, it should be noted that the multi-domain operations are very likely to be carried out at a strategic level due to the scope and diversity of the actions involved (not being entirely under the command and control of the military instrument of power) and that is why they must be taken into account.

I believe that strategic depth largely reflects what the strategic military level aims to achieve, proving its viability throughout history, achieving or maintaining it being an objective for military strategists of all time. Strategic depth refers to the distances inside a state, from its defended border to what can be considered the center of gravity of that state, to considerations related to the vulnerabilities of the center of gravity in case of war in relation to the size of the space available to stop the enemy advance, counterattack and restore balance (Khan 2015).

TABLE 1. The US Army in multi-domain operations – logic figure – from TRADOC Pamphlet 525-3-1, The US Army in Multi-Domain Operations 2028 (TRADOC 2018)

OPERATIONAL ENVIRONMENT - contested in all domains - increasingly lethal, expanded battlefield - increasingly complex environment - challenged deterrence
RUSSIAN AND CHINESE ANTI-ACCESS AND AREA DENIAL SYSTEMS CREATES MULTIPLE LAYERS OF STAND-OFF **Competition** – creating stand-off by separating the U.S. and partners politically with: - regional and national forces; - unconventional warfare; - information warfare; - long-, medium- and short-range conventional forces; in order to fracture alliances and win without a fight. **Armed conflict** – confrontation by separating the joint force in time, space and functions with: - regional and national forces; - long-, medium- and short-range conventional forces; - unconventional war; - information war; in order to win quickly with a surprise „fait accompli" campaign.
TENETS OF MULTI-DOMAIN OPERATIONS **Calibrated force posture:** - forward presence forces; - expeditionary forces; - national capabilities; - authority (to operate in all areas, especially within the competition). **Multi-domain formations:** - conduct independent maneuver; - employ cross-domain fires; - maximize human potential. **Convergence (time, space, capabilities):** - cross-domain synergy; - layered options; - mission command/disciplined initiative.
COMPETE, PENETRATE DIS-INTEGRATE, EXPLOIT AND RE-COMPETE **Competition** – to expand the competitive space - supports the defeat of informational and non-conventional war; - gathers information and counters the enemy's reconnaissance actions; - demonstrates credible deterrence. **Penetration** of strategic and operational confrontation: - neutralization of the enemy's long-range systems; - challenging the maneuvering forces of the enemy; - maneuver from operational and strategic distances. **Disintegration** of enemy A2AD systems: - defeat/destroy the enemy's long-range systems; - neutralization of the enemy's short-range systems; - performing independent maneuvers; - conduct deception. **Exploiting** freedom of maneuver to defeat the enemy: - the defeat/destruction of medium-range systems; - neutralization of the enemy's short-range systems; - maneuvers to isolate and defeat the maneuver forces of the enemy; **Re-compete** – to consolidate and extend the advantages obtained - ensuring/securing (physically) the land and the population; - facilitating lasting solutions together with partners; - establishing the conditions for long-term deterrence; - recalibration of the forces' position; - maintaining the initiative.

The problem we face, in the current security environment, is the fact that strategic depth no longer refers only to the physical (geographical) space and can have different forms that have appeared as a result of the ways of managing information and the increase of precision and strike range of the weapon systems. This is the reason why a new type of operation was needed to respond to the new developments of the concept of strategic depth, in the sense of a new idea that summarizes the current reality and what is expected to happen in the near future.

We can observe in Figure 1 above the following:
In Phase I, three of the four categories identified as elements of the cyber environment with implications in the activities carried out by the military can be found in full:

- Cyber information operations – missions in the information field - support the defeat of the information war;
- Cybercrime – crime reduction – supports the defeat of...and unconventional war;
- Facilitating the interpretation/processing of information – gathering information and countering enemy reconnaissance actions.

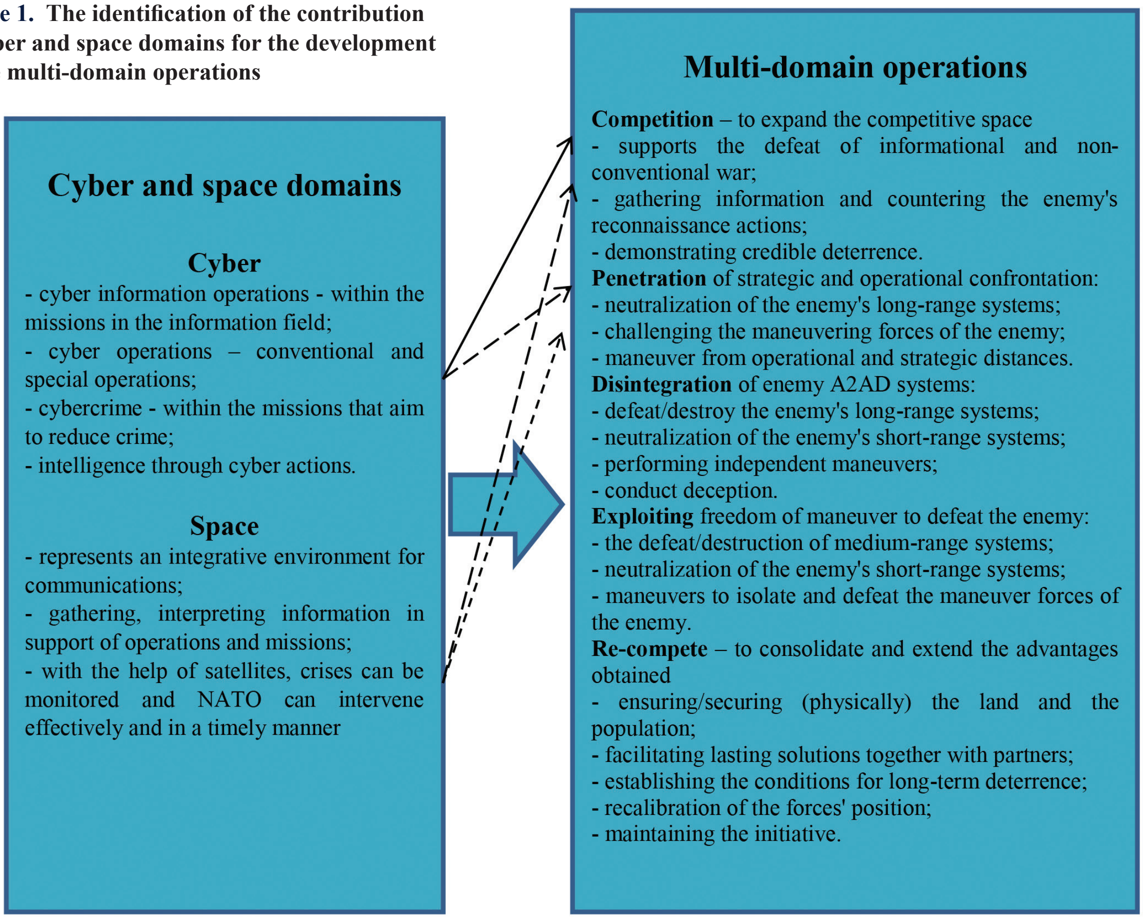
In Phases II and III, only one category (cyber operations - conventional and special operations) is found in the elements described in the two phases. In Phase II, within the maneuvers from operational and strategic distances, I consider that these cyber operations can be carried out. Later, starting with Phase III, due to the difficulties in predicting the evolution and beginning of independent maneuvers, the only aspect that can run at a centralized level from the cyber environment is deception.

The result can be interpreted from the perspective of the fact that all the elements taken into account were viewed from the perspective of the military instrument of power, the other instruments of power not being detailed, a fact that limits the analysis to the aspects managed by the military, thus the cyber instrument representing for them a force multiplier in the early stages of a conflict but which cannot substitute services or compensate for their deficiencies.

Regarding the limitation of actions in the cyber domain to the early stages of a conflict, a conclusion can be reached, which is identified in the TRADOC document in the form of the principle of the multi-domain operation – multi-domain formations – they must have elements from the cyber and space domains to converge towards the echelon, so that once the actions of the forces involved in the multi-domain operation are fragmented, they retain their coherence.

I therefore believe that what should concern the military who are in charge of the development of this concept is the identification of the ways of using the cyber and space domains within the actions specific to the services or the derivation of new tactics by the services, tactics that take into account the possibilities of using technologies from the two new environments. In this way the joint operation will be able to gain an operational advantage over the enemy even in the case of conducting

Figure 1. The identification of the contribution of cyber and space domains for the development of the multi-domain operations



Cyber and space domains

Cyber

- cyber information operations - within the missions in the information field;
- cyber operations – conventional and special operations;
- cybercrime - within the missions that aim to reduce crime;
- intelligence through cyber actions.

Space

- represents an integrative environment for communications;
- gathering, interpreting information in support of operations and missions;
- with the help of satellites, crises can be monitored and NATO can intervene effectively and in a timely manner

Multi-domain operations

Competition – to expand the competitive space
- supports the defeat of informational and non-conventional war;
- gathering information and countering the enemy's reconnaissance actions;
- demonstrating credible deterrence.

Penetration of strategic and operational confrontation:
- neutralization of the enemy's long-range systems;
- challenging the maneuvering forces of the enemy;
- maneuver from operational and strategic distances.

Disintegration of enemy A2AD systems:
- defeat/destroy the enemy's long-range systems;
- neutralization of the enemy's short-range systems;
- performing independent maneuvers;
- conduct deception.

Exploiting freedom of maneuver to defeat the enemy:
- the defeat/destruction of medium-range systems;
- neutralization of the enemy's short-range systems;
- maneuvers to isolate and defeat the maneuver forces of the enemy.

Re-compete – to consolidate and extend the advantages obtained
- ensuring/securing (physically) the land and the population;
- facilitating lasting solutions together with partners;
- establishing the conditions for long-term deterrence;
- recalibration of the forces' position;
- maintaining the initiative.

disruptive actions from the two new environments. In the case of the space domain, comparing the elements in Figure 1, it becomes even clearer than in the case of the cyber environment that gradually, within the phases of multi-domain operations, as actions become fragmented and decentralized, the relevance of actions in this environment decreases.

Regarding the last phase of multi-domain operations, I believe that its objectives can be achieved to a small extent by the military instrument of power, with other instruments of power being more suitable for this stage. Therefore, I consider that the research hypothesis that I set out to verify is partially confirmed, with the following additions:

- Actions clearly defined as belonging to the cyber and space domains are more relevant in the early phases of multi-domain operations.
- To be a determining factor in phases of open conflict, new ways of utilizing the possibilities offered by the two new environments must be identified, taking into account the specifics of each service.

However, I believe that further developments in the concept of multi-domain operations will largely depend on the willingness of state actors to engage in a new arms race.

Conclusions

By conducting the research presented in this paper, my goal was to determine the impact of two new operational environments on the development of a new concept called multi-domain operation, which aims to synthesize reality through an idea. In this regard, I described the elements that comprise the two environments and concluded that innovative technology-enabled information management represents an update of the military instrument of power, enabling the military to influence the outcome of a conflict from the early stages.

Thus, just as airspace control is essential for conducting military actions in maritime and land environments, the control of the cyber and space environments is also crucial for multi-domain operations, as all these actions represent a multi-domain operation. The fact that multi-domain operation is currently a concept under development, with an implementation horizon of 2032 for the Romanian Armed Forces, requires us to identify possible implementation methods and shortcomings.

Therefore, I believe that the multi-domain operation can be divided into three defining elements that contribute to the understanding of this new concept:

- Information management (Phase I and Phase V).
- Addressing the A2/AD issue (Phase II and Phase III).

The third issue that I introduced in this paper is the concept of strategic depth, which in my opinion is the strategic level objective that the multi-domain operation must be able to achieve, taking into account the fact that the strategic depth of the information era differs from what it represented in World War II.

Following the analysis, I noticed, first of all, the fact that the cyber and space domains gradually lose their relevance within the phases of the multi-domain operation, with the fragmentation and decentralization of actions. Later, by analyzing the correlations among the three elements, we came to the conclusion that, for the military instrument of power, the exploitation phase of the multi-domain operation is the key factor for its success. Corroborating the two conclusions, we reached the issue of implementing elements from the cyber and space environment within the services, which must be able to support the joint operations (exploitation phase). This aspect should concern the military responsible for the development of this concept, and it should lead to refining the tactics of services to include the elements that the two new environments offer.

As a result, I consider that the cyber and space domains have not yet reached their maximum potential within multi-domain operations, and the extent to which they will reach this potential is determined by the possibility of a conflict between major military powers who are willing to invest in the military applicability of new technologies specific to these two domains.

References

Comparinni, Massimo Claudio. 2022. ”Space Domain: A Global Vision.” https://www.japcc.org/articles/space-domain-a-global-vision/.

Crowther, Glenn Alexander. 2017. ”The Cyber Domain.” *The Cyber Defense Review* 2 (3): 63-78. https://www.jstor.org/stable/10.2307/26267386.

International Institute for Strategic Studies. 2015. ”Evolution of the Cyber Domain: The Implications for National and Global Security.” https://www.iiss.org/publications/strategic-dossiers/evolution-of-the-cyber-domain/chapter-one-the-1960s.

Khan, Khalid Masoon. 2015. ”The strategic depth concept.” https://www.nation.com.pk/16-Oct-2015/the-strategic-depth-concept.

NATO. 2022. ”NATO's approach to space.” https://www.nato.int/cps/en/natohq/topics_175419.htm.

—. 2016. ”Warsaw Summit Communique.” https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

presidency.ro. 2020. „Ședința Consiliului Suprem de Apărare a Țării.” https://www.presidency.ro/ro/presa/securitate-nationala-si-aparare/sedinta-consiliului-suprem-de-aparare-a-tarii1601904261.

TRADOC. 2018. ”TRADOC Pamphlet 525-3-1 – The US Army in multi-domain operations 2028.” https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf.