INFLUENCE OF CYBER DIMENSION ON AIR FORCE ACTIVITIES CASE STUDY: THE CONFLICT IN UKRAINE

Vasile-Cristian ONESIMIUC, PhD Student

"Carol I" National Defence University, Bucharest

DOI: 10.55535/RMT.2023.4.10

The cyber dimension has played an important part during the conflict in Ukraine, but the cyber activities have not had the span many military experts expected. Nevertheless, it is obvious this dimension is highly used by both sides of the conflict, and, moreover, this dimension has been active not only during the entire length of the conflict begun in 2014, but also before the annexation of the Crimean Peninsula. The increase in such activities before the start of the invasion in 2022 has done nothing else but to underline the importance of the cyber domain for future conflicts, air force security being a continuous challenge, considering that these forces are among the first ones to have been used in conflict by both Russia and Ukraine. The conflict in Ukraine has shown once more that the cyber dimension is and must be taken into consideration in each and every stage to ensure national security, before, during and after the conventional conflict, but it must not be overestimated in respect to the desired effects and those that can be achieved.

Keywords: cyber operations; conventional conflict; air force; security; risk; capabilities;

INTRODUCTION

The conflict that began in February 2022 has confirmed that air forces are among the first ones to be used for executing fighting missions against the opponent. Usually, air forces are the spearhead used for showing the military power of one state, especially for those states that do possess strong air forces. Air forces have represented and continue to be the first option with visibility and immediate impact with regards to involving military forces in military conflicts or before them, so that the adversary is forced to follow a certain course of action or to refrain from performing certain hostile actions. The early 2022 evaluations done by military experts of various states foretold a quick defeat of the Ukrainian forces, based on the size of forces and the major inequality with respect to quantity and quality of military material belonging by the two states in conflict. Therefore, more evaluations gave full credit to Russia to obtaining very fast the victory, as compared to those very few that have the courage to believe in the possibility that Ukraine resists the Russian roller for more than two weeks. Very powerful and persistent promotion of Russian armed forces led to the development of a new feeling: the hopelessness of Ukrainian resistance, the never-ending Russian military convoys from the first days of the conflict strengthening this idea.

Compared to the conventional air power where things appear quite clear, in the sense that states which hold modern air forces, with latest aircrafts can impose a certain behaviour to those states that do not hold air forces that are developed enough in number and the quality of fighting aircraft, the cyber dimension of air operations has fewer clear aspects. Therefore, a scientific analysis to further approach this subject is needed, in order to identify improvement methods so that cyber security can be ensured for air forces activities.

Considering this, the research intends to provide an answer to the question of whether cyber domain is important and still topical for the activity of air forces, bearing in mind the evolutions registered during the conflict in Ukraine. In this sense, the purpose of this article is to identify, based on the available open sources found, how the cyber domain has been integrated into the activity of air forces, considering the evaluations performed before and during the conflict in Ukraine. The questions posed in the beginning for this analysis were:

- Will we find a cyber dimension to future conflicts?
- Is this dimension going to be important for the activities currently being performed and if yes, how important will it be?
- Should we approach the integration of cyber aspects from ensuring cyber security as a whole, or, rather, it should be centred on solely ensuring the cyber aspects of a mission?

TRANSITION FROM CYBERSECURITY AS A WHOLE TO ENSURING THE MISSION

Unlike other states that are well cyber developed, Russia did not look for publicity with respect to its performed actions, and usually does perform cyber actions as hidden as possible (Caimeanu, 2021), so as not to leave traces or reveal the interest for certain targeted objectives. However, the cyber attacks are not so anonymous as one might think, and Russian links with cyber attacks performed even upon NATO states as well as upon non-NATO ones were identified, such as for example Estonia in 2007, Georgia in 2008, Ukraine beginning with 2014, Montenegro in 2016, France in 2017, to mention only a few from those that were identified.

US Cyber Command (USCYBERCOM) stated as early as 2018 that cyber actions performed by opponents were done under the threshold of armed conflicts in order to weaken the state institutions and to take the initiative on strategy level (https://assets.documentcloud.org/documents/4419681/Command-Vision-for-SCYBERCOM).

The Ukrainian authorities appear to have taken seriously what the American military forces have said, and, consequently, the following fights within cyberspace have not had the results intended by Russia. For example, the 2015 attack over Ukraine's energy network, allegedly attributed to Russian hackers, attack that also affected air transport facilities, was re-done in 2016, but with less intense effects than the precedent one (Timea, Skopik, 2018, p. 43). From the Russian Federation point of view, Russian armed forces are in two stages – war or preparing for war, and the political ambitions of the leaders have received support by means of new possibilities to fight without officially declaring war, the instruments such as cyber attacks being considered as central elements to performing and winning contemporary conflicts (Lilly, 2022, p. 17).

ADVERSARIES OPERATE CONTINUOUSLY
BELOW THE THRESHOLD OF ARMED CONFLICT
TO WEAKEN OUR INSTITUTIONS
AND GAIN STRATEGIC ADVANTAGES

Source: Command-Vision-for-USCYBERCOM-23-Mar-18

One cannot disregard the influence the cyber dimension has over the activity of the air forces, even if it is rather difficult to measure. Following this line, the lack of accountability for cyber actions may lead for cyber domain to a lesser possibility to being comprehended, as well as its intended purposes or those able to be obtained, from the attacker's and the defender's perspectives.

The most difficult to solve problem with respect to the cyber dimension is the plethora of current challenges, even if progress is being made in some parts, because they are rapidly analysed by the opponent to prevail itself of the advantage of the offensive over defence. In the above-mentioned report, the experts have estimated that the Russian cyber groups have evaluated the result of the cyber activities performed and have made adjustments to the cyber weaponry to obtain the desired effects.

One of the biggest challenges of the cyber domain with regard to aviation operations is the persistence of cyber campaigns performed by a strong opponent that is very well developed in cyber area. These cyber campaigns, which do not have immediate effects to be very visible, pass *"under the radar"* of the entities that have as responsibility to ensure cyber defence, but, in time, this apparently harmless activity can significantly erode the air force, having generalized effects.

The war in Ukraine has shown that an opponent did not manage to use the cyber dimension to organize the performance of big cyber attacks to such extent to neutralize the air force so that it cannot respond to the conventional attack. What was noticed is that the cyber attacks have not been devastating, not enough to neutralize the forces of the opponent, thus it became obvious that a conjugated intervention was needed – cyber and classic with conventional weapons.

The conflict from Ukraine was not in this respect similar to the Israeli action in Syria. The cyber dimension does not provide us with a universal tool able to neutralize enemy's forces, so as there will be no need for conventional actions being carried out. In the case of Israel, the cyber dimension was used to support and facilitate aerial actions. After the performance of a cyber-attack that disabled the Syrian air defence at right time and place, there followed the conventional action of bombing the targeted objectives. The differences between the two cases are quite important; firstly, between the two states there was no conventional war in progress, and the cyber issue was not so vividly debated, we could say that there was pretty primitive approach to a serious cyber defence.

James Cummins (2022, p. 73) identified the need to consider cyber domain as a big issue for the air force, not only for their IT component, thus raising the relevance of this domain for NATO military commanders. Even for the *"simplest"* missions carried out during times of peace, ensuring air policing service, cyber domain has a special importance, all interactions being complex, beginning with monitoring the air space, the decision-making process within short notice, decision to take off for aircraft in order to control the situations where there are detected some trespassing of the air space and up to the completion of the mission of the aircraft, namely ensuring continuous control. Cummins justifies the need to consider cyber domain as an overall problem of the mission by two aspects: both the complexity of the mission itself, and the fact that components of the cyber domain from outside NATO cyberspace are being used, here being included national networks, civil infrastructure and information systems from abord aircraft and their operating bases.

Ensuring cyber security with focus on the mission (Ib.) brings more benefits to the decision-making process when performing a mission, by a better understanding of the operating environment, the cyber threats and risks for the mission. Understanding the way cyber threats and vulnerabilities do contribute to rising the risks when performing a mission, leads to a more effective application of cyber effects, whereas this interaction between the mission and the cyber space introduces the need for cyber operations executed to support the performance of the mission. Understanding the air context as support to perform the mission has traditionally put the focus on the network components that exist physically and less to virtual part, which is more difficult to conceptualize. From cyber domain, commanders need to be able to predict which of the changes from within cyberspace might jeopardize performing future missions, considering both one's own actions, and those of the opponent.

CASE STUDY: CONFLICT IN UKRAINE

Cyber attacks have been the newest instruments identified as used by Russia. In this case, it was very easy for Russia to consider cyberspace as being an extension to its territorial borders (Caimeanu). From this point of view, one cannot see big differences regarding Russia's cyber policy as compared to how it regards Ukraine physically; in both cases, Russia intends to cross the borders as they have been officially recognized between them and to illegally take over new territories that do not belong to it.

Jakub Przetacznik (2022) has concluded a report for the European Parliament where he analyses the cyber activities performed by Russia over Ukraine. Within the report, it is underlined that although Russia started the war against Ukraine on 24 February 2022, the Russian cyber activities had been continuously performed from 2014 when Crimea was annexed and intensified before the invasion of February 2022. Cyber actions with visible effects targeted different elements of Ukrainian infrastructure, but there were surely performed cyber activities that aimed for unauthorized access to Ukrainian intelligence systems, as well as to gathering data and information.

One hour before the invasion started, a cyber-attack on satellite communication system was executed, attack which led to disruptions in ensuring communications for natural persons, as well as for Ukrainian legal private and public entities. Also, there were carried out attacks that targeted electrical energy networks, attempts to destroy or disturb governmental agencies networks, in some cases performing also rocket attacks on targeted objectives, aiming, most likely, to undermine Ukraine' political will and its fighting ability, while collecting information that may bring tactical or strategical advantages to the Russian forces (Lapienyte, 2022). Approximately 40% of the attacks that caused damages to the inner Ukrainian infrastructure targeted organizations from critical infrastructure, which may have had collateral negative effects on government, army, economy and population, at national, regional or city levels (Microsoft report, 2022, pp. 2-3). According to the data in the said report, Microsoft estimates that the activities of Russian groups, which prepositioned within cyber area as part of the conflict preparations, began the previous year, the cyber activity aiming to secure access for gathering intel on strategic and operational level as well as to facilitate attacks over Ukrainian infrastructure during the military conflict (Ib., p. 4).

The performed cyber attacks had targets in both Ukraine and abroad, including from within NATO member countries, the activity performed during 2021 being spying at a larger scale. Beginning with 2022, cyber destructive activity intensified and reached a peak of cyber activities before the invasion started, malware specially developed for targeted systems being inserted into Ukrainian systems.

Once the invasion began, identified Russian cyber activity has performed missions to support strategic and tactical military targets, but without being very clear whether there has been some coordination, centralized tasks or a common set of priorities (Grossman, Kaminska, Shires, Smeets, 2023, p. 11). In some cases, the cyber attacks have been executed before a conventional military attack, but these cases appear to be rare. The cyber actions were meant to either destroying, disturbing or discrediting the Ukrainian government, army, companies or critical infrastructure. On 6 March, Russian armed forces launched eight missiles against Vinnytsia airport, whilst prior to this, on 4 March, a cyber-attack had compromised governmental air networks used in Vinnytsia (Microsoft report, p. 7).

Analysing available data turned out that Russian groups acted within the same geographical areas or points where kinetical military strikes were performed, for the first six weeks of the invasion.

Contrary to the expected, in the first stages of the war between Ukraine and Russia, although most of the experts thought cyber actions would be playing a bigger part within fighting action, there were not observed any intense cyber activities. The Microsoft report presents most of these cyber activities, without claiming to be complete. Most of the experts support the evaluation according to which, in order to understand the magnitude of the cyber actions, this war must be brought to an end and a certain period of time to pass to a greater reveal on how the events succeeded. Nevertheless, it is obvious that without consulting both parties currently in conflict, it seems rather unlikely that both the Ukrainian part as well as the Russian one to be willing to share really sensitive elements of the actions that were performed.

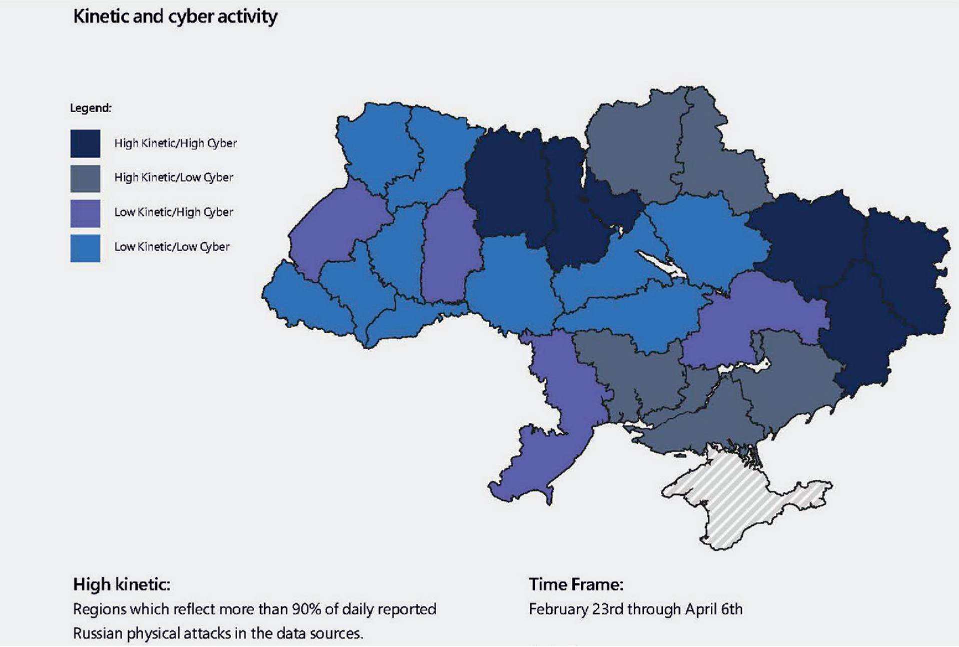
Kinetic and cyber activity
Legend:
High Kinetic/High Cyber
High Kinetic/Low Cyber
Low Kinetic/High Cyber
Low Kinetic/Low Cyber
High kinetic:
Regions which reflect more than 90% of daily reported Russian physical attacks in the data sources.
Time Frame:
February 23rd through April 6th

Figure 2: Correlation between cyber activities and conventional military actions (Ib., p. 9)

The development of digital infrastructure has allowed access to top-level technology much easier than in the case of aviation. It is understandable why such access to the top-level technology in aviation is being protected, both in terms of economy and especially statal security, in order to maintain technological advance towards potential opponents. Large-scale use of digital infrastructure in numerous domains, even if in this case there are restrictions to access latest technology, has allowed for a wider spread compared to air force niche one.

Air forces carry out their activities so as to be able to perform the assigned missions, but also to manage future threats associated to operation in contested environments, both conventionally and cyber. It implies a continuous sustained effort, upon all levels, for the fighting forces and mostly for the commanders. Changing the way people think is a difficult lengthy process that is extremely necessary in the context of rapidly developing security environment.

Due to the need to protect the Ukrainian air force, considering the superiority of the Russian air forces the Ukrainian leaders have decided to send off the forces and the means both to the main airfields and to spare locations. Therefore, the need to ensure cyber security differently than the one at the level of the air base, in a centralized manner. In my opinion, moving from ensuring cyber security as a whole to ensuring the mission has been done naturally, following the shortening of forces and resources from the spare locations. At tactical level, flight missions mean taking decisions extremely fast based upon information that more often than not is incomplete and that can later either prove to have been good or, on the contrary, to have been bad. From this point of view, cyber dimension is very important, at tactical level the commanders can use other options to try solving a situation that usually would require performance of a conventional offensive action.

From a strategic point of view, the cyber dimension is very dynamic and contested, evolutions of the civil cyber domain being used also by the military, the differences from cyber domain being much or easier to cover than in the aviation domain. Putting up conventional air forces requires more time and resources than for cyber domain. The cyber dimension can be used together with other military capabilities, and it determines the increasing attractivity of this domain, considering the perspective of the results that could be achieved and the lower risk level as compared with classical offensive air operation. Beginning with ensuring the mission and thus the aircraft or the pack of aircrafts used, the Ukrainian air force have built cyber security as a whole, an approach adapted to the strategic available needs, but also adjusted to the tactical realities.

The conflict in Ukraine has clearly proven that future confrontations shall include a cyber dimension. The Microsoft report, even having incomplete data gathered or accessed by the experts during their stay in Ukraine, shows that the cyber dimension was employed before the conventional conflict began. Cyber activities did not stop after the hostile takeover of the Crimean Peninsula in 2014, the growth of cyber activity being signalled many months before the conventional attack started in February 2022. The increased attacks did not come as a surprise, both NATO and Ukraine being aware that the cyber dimension shall form an integral part of this conflict. Nations that have weaker conventional military capacities may use the cyber component as a forceful multiplier against nations that are more powerful in military, economic and industrial capacities (Stoddart, 2022, p. 29).

INTEGRATING CYBER DIMENSION INTO THE PLANNING PROCESS DURING THE CONFLICT

A strong cyber force can help small armed forces to resist with success to a stronger power. The serious analysis of threats in the cyber domain by Ukraine, conjugated with the very intense foreign support (Cyber Peace Institute, 2023, pp. 15-17) from EU, NATO and other non-state players, more or less developed, has allowed the creation of a cyber defence comparable to that of the attacker.

This defence was not instantly created, resources and sustained efforts were needed to achieve it. The race to arming had to consider, during all stages of the conflict, from planning, performance, desired effects and achieved effects, the integration of the cyber dimension, from the attacker's perspective and the defender's one.

Planning

Integration of the cyber domain into the planning of aerial operations had to take account both own forces as well as those of the opponent, the intended missions, possible courses of action, support with intel and, last but not least, the conflict dynamics. A simple list of elements to be considered during planning aerial operations show the magnitude of the problems that need to be solved. Both parties in conflict have considered objectives that are strategically very different. By an initial planning, it appeared that the Russians planned a fast conflict and, consequently, the performed cyber activities have focused especially on showing certain capabilities to imprint a certain course of action from the Ukrainians. It is likely that during the initial stage of the conflict, there could not have been properly evaluated the defensive cyber capabilities Ukraine had; similar to conventional military forces, Russia did not believe the Ukrainian cyber forces are comparable to the Russian ones, considering the history of cyber activities between the two forces, the freedom of manoeuvre of the Russian cyber groups operating on Ukrainian systems giving them permission to perform cyber activities quite easily.

Performance

If with respect to aerial domain, neutralizing a target by using conventional means can be evaluated due to the visibility of the damages caused by using kinetical weapons, in cyber area, certifying the fact that an adversary system has been neutralized by using cyber weapons is more difficult. Success in cyber area can be permanent, just like when using conventional weaponry, but it can be only temporary, therefore it would be beneficial if there could be other ways to confirm success for a cyber operation.

In our case, Ukraine has managed to integrate very efficiently the foreign help it received from the international partners, as the conflict unfolded, and it blocked the cyber activities of the opponent. Moreover, whenever this could not have been done, it managed to block its initiatives to confirm the effects of cyber attacks. Later on, as a result of not being able to obtain the intended results by the Russian counterpart by means of the cyber dimension, the Russian air force went on to missions of conventional bombing over targets of the Ukrainian air force.

Intended effects

Considering the intended effects, there should be a very precise coordination to integrate the cyber dimension into air force operations and a coordination with the other areas: ground, maritime, which could simultaneously act and interact for achieving the desired effects. From this point of view, the deconfliction at specialists' level, but also at commanders' level is needed. The issue is of rather complex and difficult nature, the intended effects can be at strategic, operational or tactical level. The higher the level, the more likely is that the cyber dimension within the air force disturb or be disturbed by actions of other domains. From the Ukrainian perspective, coordination regarding the intended effects was easier to be done, the forces command was unitary, unlike the Russian counterpart where different state and non-state cyber entities were involved. At least in the first part of the conflict, Russian entities have acted chaotically, without an efficient coordination achieved considering the intended effects and the way they could be achieved.

Results achieved

The conflict in Ukraine has proven how hard it is to perform a joint operation through many action directions. Moreover, the inclusion of the cyber dimension poses new challenges with respect to the results achieved, considering including the cyber dimension into the joint operation. The cyber dimension must ensure national security from a cyber point of view and perform offensive cyber actions against facilities and infrastructure the adversary possesses.

The intended effect by the Russian part at the beginning of the conflict have not been obtained. Even with little information available, one can notice there was a transition from performance of Russian cyber attacks over Ukrainian facilities to a Ukrainian reply over Russian facilities. It can indicate growth of Ukrainian cyber defence, which now feels more confident to defend from a cyber point of view its infrastructure and performs even offensive action, to support the offensive actions of its military forces. The offensive cyber actions performed by Ukraine can detour Russian forces and means from performing offensive actions to defensive actions, moving the focus on the protection of facilities and infrastructure upon Russian national territory.

As to the results achieved, there has been noticed the tendency to symmetrically react to the actions of the opponent, and also to use the evaluated means as being the proper ones to reply by means of conventional attacks and also cyber attacks, irrespective of the attack method chosen by the adversary.

Ukraine has shown a great deal of skill in using all available means to protect its national territory. The contribution of the cyber dimension to the continuation of mission performance by Ukrainian forces cannot be evaluated at its true value, but it can be easily said that the cyber domain is one of the pillars supporting the security of the Ukrainian air force and, thus, the provision of national security for Ukraine. Even if at international level Ukraine was situated way below Russia as regards cyber area, it managed in the short time available and under pressure of a continuous war, with substantial foreign support, to build a cyber defence able to face the Russian threat.

CONCLUSIONS

Air force is by default using high-end technology which have implemented the latest innovations of various areas very soon form their issuance. Consequently, the air force, as a leader in innovation, has confirmed pretty soon the importance of cyber domain to both their defensive and offensive activities. The cyber domain has brought a number of advantages to air force, at the same time bringing new vulnerabilities and associated risks. Approaching cyber security through military perspective, which starts from the strategic level to the tactical one with respect to ensuring protection of critical infrastructure is slightly different from the private perspective which considers the protection of critical infrastructure from an economic point. Therefore, the influence of cyber domain over air forces cannot be regarded as only military, or only civil, but rather, it needs to be considered that malicious cyber actions are the result of the activities of hostile state(s). In other words, ensuring security for the critical infrastructure of the air force has a direct connection to ensuring national security, by allowing the air force to operate for protecting national air space. In my opinion, cyber domain is important and topical for the activities of air forces, the case study proving it. Moreover, it is necessary an adjustment to the way it is being considered when ensuring the mission as central element of cyber security.

Limited resources, as well as their assignment to solving the problems considered to be urgent, have led constraints for cyber domain, the very existence of a structure meant to cyber defence has been considered good enough.

However, the Ukrainian conflict has shown that, although the importance of the cyber domain has been recognized and there have been initiatives to ensure cyber defence, it was not enough. As being underlined in the Microsoft file, hostile cyber actors/players have exploited much more efficiently the cyber domain, the malware cyber activity has been at high levels most of time, as proved by the impact of the completed cyber attacks. For a cyber state actor/player such as Russia, a sustained effort for Ukraine was needed, and it has been given a boost by the urgent needs of the war to reach a satisfactory level for cyber security. It becomes obvious that cyber dimension shall be a component of future conflicts, and, I believe that, due to an ever more evolving technological advance, the place and importance of the cyber dimension shall gradually grow within the activities of the air forces, so that air forces survive.

The impossibility to ensure air supremacy for the Russian forces, even if there has been an intense activity in the cyber domain and for longer intervals of time, has proved once again the importance of assuring a strong efficient defence. In other words, we should not overestimate expectations towards the defensive and offensive cyber capacities, the conflict demonstrating that there are some limits related to what can be achieved. Nevertheless, as shown by the war between Ukraine and Russia, the cyber dimension contributes to ensure the security of the Ukrainian air force and nation and will continue to be an important part, even mostly unseen, of the conflict.

It is rather fair to say that the focus the Ukrainian air force had on protecting missions from a cyber point of view, whilst high levels of risk were generally accepted as reasonable, allowed the flight missions to be continued during the conflict between the two states. As it has already, and, still is, being proved by the war between Russia and Ukraine, the influence of cyber dimension over the activity of the Ukrainian air force cannot be neglected, its contribution to ensuring national security for Ukraine being thus implicit.

BIBLIOGRAPHY:

1. *An overview of Russia's cyberattack activity in Ukraine. Special Report Ukraine, Microsoft* (2022), pp. 2-3, https://aka.ms/ukrainespecialreport, retrieved on 10 June 2023.
2. Caimeanu, M. (2021). *A cincea dimensiune. Rolul spațiului cibernetic în gândirea strategică a Federației Ruse*, http://ispri.ro/a-cincea-dimensiune-rolul-spatiului-cibernetic-in-gandirea-strategica-a-federatiei-ruse/, retrieved on 9 June 2023.
3. Cummins, J. (2022). *Addressing Cyber Challenges Through the Prism of The NATO Air Policing Mission*, https://www.jwc.nato.int/newsroom/The-Three-Swords-Magazine/three-swords-38, retrieved on 28 September 2023.
4. Cyber Peace Institute (2023). *Cyber Dimensions of the Armed Conflict in Ukraine, Quarterly Analysis Report Q1 January to March 2023*, https://cyberpeaceinstitute.org/wp-content/uploads/2023/05/Ukraine-Report-Q1_FINAL.pdf, retrieved on 11 June 2023.

5. Grossman, T., Kaminska, M., Shires, J., Smeets, M. (2023). *The Cyber Dimensions of the Russia-Ukraine War,* https://eccri.eu/wp-content/uploads/2023/04/ECCRI_REPORT_The-Cyber-Dimensions-of-the-Russia-Ukraine-War-19042023.pdf., retrieved on 10 June 2023.
6. Lapienyte, J. (2022). *Russia correlates cyberattacks with its kinetic military operations in Ukraine – Microsoft, 2022,* https://cybernews.com/cyber-war/russia-correlates-cyberattacks-with-its-kinetic-military-operations-in-ukraine-microsoft/, retrieved on 9 June 2023.
7. Lilly, B. (2022). *Russian Information Warfare: Assault on Democracies in the Cyber Wild West*, Naval Institute Press,
8. Microsoft (2022). *An overview of Russia's cyberattack activity in Ukraine, Special Report Ukraine, Microsoft*, https://aka.ms/ukrainespecialreport, retrieved on 9 June 2023.
9. Przetacznik, J. (2022). *Războiul Rusiei împotriva Ucrainei: Cronologia atacurilor cibernetice*, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(202)733549, retrieved on 6 June 2023.
10. Raffray, E., Millochau, G. (2023). *War in Ukraine computer network control and impact on civilians*, https://cyberpeaceinstitute.org/publications/war-in-ukraine-computer-network-control-and-impact-on-civilians/, retrieved on 11 June 2023.
11. Stoddart, K. (2022). *Cyberwarfare, Threats to Critical Infrastructure*. Editura Palgrave Macmillan.
12. Timea, P., Skopik, F. (2018). *Collaborative Cyber Threat Intelligence.* Editura CRC Press.
13. https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM23-Mar-18.pdf, p. 3, retrieved on 18 September 2023.