THE RUSSIAN-UKRAINIAN WAR AND ITS IMPACT ON CYBER SECURITY IN NATO AND THE EU

Lieutenant Colonel Claudiu-Cosmin RADU, PhD Candidate

"Carol I" National Defence University, Bucharest

DOI: 10.55535/RMT.2023.4.1

Since early 2022, before the outbreak of the Russian-Ukrainian conflict, cyberspace has been extensively utilised, with cyber operations playing a pivotal role in information concealment, deception, and attacks on critical infrastructure. Warfare has evolved, growing more intricate, and the amalgamation of cyber actions with hard power effects is progressively causing greater disruption. Cyber actions have extended beyond Ukraine's borders, influencing neighbouring NATO and EU member states. These incidents are as pertinent as they are perilous for the security of states on the eastern flank of the North Atlantic Alliance. This article explores the imperative for alliance cooperation and the development of cyber capabilities, doctrines, and strategies to foster a security environment conducive to the region. As a NATO and EU member state situated on the Eastern flank, Romania must remain a bastion of stability and a provider of security in the region. The alliances Romania is part of must adapt to confront these challenges.

Keywords: cyberspace; Russian-Ukrainian war; cyber operations; cyber security;

INTRODUCTION

The Black Sea region has become an area of global concern characterised by a high potential for instability since the outbreak of the conflict between the Russian Federation and Ukraine. The security vision of the states in the region is strongly influenced by the aggressiveness of the Russian Federation, and, as a result, Romania's role in ensuring the security of both the North Atlantic Alliance and the European Union has become very important. The presence of foreign military forces on its territory and joint exercises with the allies aim to reassure the population, which must regain a more positive perception of its security more quickly.

The desire for a stronger military presence is natural, given that the threat stems from a superpower that has historically held influence over this region. From the perspective of an assertive Russia, the additional allied military presence on NATO's eastern border is not of significant concern. Even though the actions in the conflict are primarily kinetic, there are implications from both sides regarding cyber issues. The latter typically involves covert or deceptive operations aimed at coercing the adversary. More recently, cyber operations serve as both complementary activities in warfare and decisive actions in their own right. Essentially, the Russian Federation is using Ukraine as a shooting range to enhance its cyber capabilities by experimenting with and operationalising various new methods. Additionally, the Russian Federation is employing hybrid methods of attack that have been tested in other conflicts, as cyber attacks continue to evolve in sophistication.

Like other states, Romania has a fundamental role to play in securing the eastern border of NATO and the EU. Romania has agreed with NATO and aims to become a vector of stability, democracy and Euro-Atlantic values in the Black Sea region. Romania has the ambition to become a pillar of regional geopolitical security and has the opportunity to establish itself as an excellent security provider. As an active member of the North Atlantic Alliance and the European Union, it has a long-term commitment to investing in security, promoting peace and stability, expanding the market economy, embracing the values that characterise a society open towards the West, and engaging with strategic partners.

As the war in Ukraine progresses, Russian agencies are focusing their cyber-influence operations on the Ukrainian population to undermine confidence in the country's will and ability to resist Russian attacks. In addition, the Russian population is targeted by the propaganda because their support is needed to sustain the war effort. Kyiv-supporting states have also been the targets of cyber attacks aimed at warning and deterring. Most of the attention on cyber attacks as a component of war focuses on the potential to disrupt, degrade or destroy targets. However, the Russian Federation has an extensive history of using network intrusions to gather intelligence, and these operations can be much harder to detect.

An important lesson learned from the deployment of multi-domain task forces is the exemplary mobilisation of other states in support of Ukraine. This can certainly lead to better inter-state cooperation within the North Atlantic Alliance and the European Union, laying the foundations for a new form of collective defence. Ukraine has also benefited from a great deal of support from private entities: leading companies in the cyber security market, groups of renowned hackers as well as groups of patriotic volunteer hackers. In general, cyber attacks, as components of warfare, can disrupt, degrade or destroy critical infrastructure. Moreover, the Russian Federation has an extensive history of using network intrusions to gather intelligence, spy, degrade or block adversary systems. These actions can have immediate effects or be launched to produce effects over time without detection.

RUSSIAN FEDERATION'S INFORMATION WARFARE BEFORE 2022

To better understand operations in the cyber environment in Russia's military actions in Ukraine in early 2022, one should consider Moscow's unique way of viewing cyber operations and applying doctrines to achieve success on the battlefield. However, in this article, I will not analyse the doctrinal aspects of cyber actions but will focus on how these actions play out in the cyber environment. I will also research the effects that these actions generate, to identify a pattern in the use of these cyber attacks by the Russian Federation.

One of the main results of the rapid development of information technology has been that it has moved traditional confrontations into the virtual environment, creating alternative spaces to reality. Cyberspace has become a new battlefield, characterised by its increased speed and efficiency compared to traditional methods of combat. A significant advantage of this environment is that the risk of loss of life is minimal. This new domain of confrontation was officially recognised as a domain of operations by members of the North Atlantic Alliance at the 2016 Summit in Warsaw, Poland (North Atlantic Treaty Organization, 2023).

The Russian Federation used this domain of confrontation much earlier, but as we can see even today, its strategy is to use conventional warfare combined with non-kinetic actions such as propaganda, espionage, cyber-terrorism, cyber-operations and the use of malware. These types of attacks used on information and information systems are designed to mislead the population, disrupt economic activities, disable critical national infrastructure, and gather intelligence on military capabilities and vulnerability to the security of the target state. The Russian Federation has been known as an actor capable of carrying out a wide range of cyber espionage and sabotage operations since the 1990s (Aliyev, 2022). It already has extensive experience in the information environment, based on the disinformation campaigns coordinated by the government itself, with which it managed to mobilise the ethnic Russian population in 1999 during the second war with Chechnya, using the media as a means of propaganda.

Another campaign of cyber attacks, this time of greater scale and resonance, was the series of cyber attacks in 2007 against Estonia, amid historical disagreements between the two countries. For several days, cyber attacks were carried out against several Estonian targets such as the websites of ministries, banks, political parties, media and telecommunication services. The effects were surprising, as Estonia was a fairly digitised country at the time (Herzog, 2011, p. 51). Those attacks, which were to block various Estonian targets for a limited period, reconfirmed Russian capabilities in the information environment. Becoming the first country to face a cyber attack of such magnitude, Estonia needed external help from allies and the international community. A year later, the Russian Federation used hybrid methods of action in the Russian-Georgian war. Non-kinetic actions consisted of cyber attacks and psychological intelligence, including propaganda and fake news. Georgia, a country seeking democratic success in the West, moving ever closer to the US and NATO, sparked Russian discontent. It resorted to military action against Georgia after the 2008 NATO summit in Bucharest, where the allies discussed with the government in Tbilisi the possibility of joining the North Atlantic Alliance. Even if the talks did not lead to a concrete result, the change in ideology and attitude towards the Kremlin and the rapprochement with the Euro-Atlantic area increased Russia's aggression towards this small state.

Since the same year, public support for Georgia's European and Euro-Atlantic integration has grown strongly. According to a recent poll conducted by the National Democratic Institute (NDI) in 2021, 80% of Georgians expressed support for Georgia's EU membership (up from 76% in 2020), while 74% of the population supported

NATO integration (up from 69% in 2020) (Seskuria, 2021). At the time, the Russian security services managed to dominate the information domain through techniques and means of information manipulation that included propaganda, information control and disinformation campaigns. Part of the Kremlin's propaganda increasingly focused on changing public opinion, claiming that the Russian Federation was the determining factor in regional security and conflict cessation and that Western states had neither the capacity nor the interest to do so. Spreading anti-Western news through local actors actively cultivated and financially supported pro-Russian parties and spread ultra-nationalist and xenophobic messages (Seskuria). Through television broadcasts and daily interviews with a military spokesman, the Russian Federation controlled the international flow of information and tried to influence local populations by pushing news, disseminating the progress of Russian troops protecting Russian citizens and highlighting Georgian atrocities (Iasiello, 2017, p. 53). Moreover, actions in the cyber environment ran concurrently with physical military operations, so that they led to defacements of websites, denial of service and distributed denial of service attacks against the Georgian government, Georgian media and financial institutions, as well as other public and private actions. The attacks succeeded in denying citizens access to 54 websites related to communications, finance and government (Iasiello, 2017, p. 52).

Later, between 2011 and 2013, the protests caused by the controversial elections in the Russian Federation demonstrated how the media could be used to manipulate the population to generate waves of public discontent. These, along with the Arab Spring, demonstrate the effectiveness of social media in changing regimes. Moreover, they helped the Kremlin government develop information capabilities that facilitated the annexation of Crimea in 2014. In this context, cyber tactics, techniques and actions resulted in the disruption of government information networks, paralysis of the command-and-control system, disruption of communication channels and served as tools to reinforce hybrid warfare strategies. Psychological operations played a crucial role in amplifying the effectiveness of these strategies. Gradually, psychological operations began by trying to gain credibility and persuasion among individuals, then focused on exerting pressure on the population in Crimea and Ukraine. Ultimately, the aim was to create conditions that would minimise the image of the Russian Federation as an aggressor state. Ukraine's response to this hybrid conflict was characterised by inadequate and fragmented reactions, with a dominance in the informational, virtual media and psychological spheres (Stanciu, 2016, p. 74).

In my opinion, the Russian Federation studied previous conflicts, and applied the lessons learned so that they synchronised kinetic and cyber attacks. The latter were considered essential strikes with maximum effectiveness especially on critical infrastructure. These Russian cyber operations were aimed at disabling Ukraine's digital infrastructure, disseminating pro-Russian propaganda and breaking the will to fight among political, military and civilian leaders alike. The cyber actions were also aimed at discouraging Ukrainian allies from intervening in the conflict. Russian state and non-state cyber actors coordinated a series of denial-of-service (DDoS) attacks on Ukrainian government websites, targeting, in particular, politicians believed to hold anti-Russian views and election-related websites. Moreover, they aggressively spread various pro-Russian propaganda and fake news on Ukrainian social media platforms (Salt & Sobchuk, 2021, p. 1). We can certainly affirm that the Russian Federation used this conflict as an opportunity to test its new cyber techniques, tactics and procedures and to further improve these capabilities by testing and operationalising various new methods. Cyber attacks against Crimea shut down telecommunications, disabled major Ukrainian websites and blocked the mobile phones of key Ukrainian officials before Russian forces entered the peninsula (Iasiello, p. 54). With this conflict, cyber attacks evolved from propaganda to actual disruption of physical infrastructure, such as destabilising the Ukrainian power grid and causing blackouts across the country. Such cyber attacks occurred on an industrial scale, sometimes reaching several thousand per month. Attacks also mainly targeted private sector companies with malware, further complicating Ukrainian attempts at cyber defence, as many computer systems became infected with Russian malware without detection.

The Russian Federation's cyber operations influenced the fighting on the ground even at the tactical level. The Russians were able to use various technologies to discover and transmit messages on the mobile phones of both soldiers and their families, intending to make them give up fighting. The fact that most personal and even company computers had outdated security systems made them vulnerable. These waves of Russian cyber attacks are more like bombings than precision strikes, designed to overwhelm any Ukrainian defences and countermeasures (Salt & Sobchuk, p. 2).

US military experts said the cyber attacks were undoubtedly carried out to isolate Crimea and facilitate troop movements into Ukrainian territory. However, even after the conflict ended with the annexation of Crimea to the Russian Federation, state and non-state actors with pro-Russian affinities continued their activities in cyberspace even in peacetime. These cyber activities were aimed at testing the vulnerabilities of Ukrainian systems, and in this way Russian cyber specialists trained for future cyber attacks.

The Russian Federation also carries out cyber attacks in the absence of planned military action, trying to disrupt the policy of other states by not wanting to provoke an armed war. Elections, in general, can be extremely vulnerable, as they offer external actors the chance not only to support a preferred candidate but also to raise questions about the integrity of candidates and the fairness of the electoral process. The interference in the 2016 US presidential election is the best example of the Russian Federation's use of information-technical and information-psychological techniques. This took the form of collecting and subsequently leaking data from party registers, as well as the personal data of some candidates. There have also been specific data collection operations and cyber incidents related to elections in the European Parliament, Ukraine, Sweden, France and other countries. These are defined by spear-phishing campaigns to access data, hacking operations and information leaks, disruptive attacks on electoral infrastructure, and the use of the online environment to spread false information and manipulation (Hakala, Melnychuk, 2021, p. 27).

Given the above, we can say that the Russian Federation uses numerous cyber attacks to destabilise, disable or hamper critical communications systems and infrastructure. On the propaganda and disinformation side, it has very well developed systems. Actions in the information environment are underpinned by numerous strategies and doctrines, including the controversial *"Gerasimov Doctrine"*. Russia's actions in cyberspace are designed to prepare the battlefield before introducing troops or using conventional weapons. Essentially, it uses the most dangerous cyber attacks on the critical systems of the country it is about to attack to cripple it.

RUSSIAN-UKRAINIAN WAR 2022 – CYBER ASPECTS

In January 2022, after a large concentration of troops on the border with Ukraine, the Russian Federation demanded legal guarantees from the United States and NATO member countries that Ukraine would not be accepted to join the North Atlantic Alliance. After the demands were refused, a month later satellite images showed an impressive deployment of Russian ground forces and helicopters on the Ukrainian border. The next move was to withdraw all diplomatic personnel from Ukrainian territory, indicating preparations for a military operation against the neighbouring state. Thus, the Russian military crossed the Ukrainian border on 24 February 2022 in a combined offensive of troops, tanks, planes and cruise missiles in what the Kremlin called a *"special military operation"*, demonstrating that it would not allow Ukraine to be outside the Russian sphere of influence.

Ukraine's eventual accession to the Western military alliance would represent a change in the regional geostrategic and security situation and would be seen as a threat to Russia's interests and security, practically bordering directly on NATO. This Russian military offensive led to the largest mobilisation of military personnel, weapons and equipment in Europe on the battlefields since the Second World War (Guchua, Zedelashvili, Giorgadze, 2022, p. 30).

However, the first *"missiles"* were launched on 23 February, hours before the rockets were launched or the tanks moved. This was a new round of offensive and destructive cyber attacks directed against Ukraine's digital infrastructure. Microsoft has detected and notified Ukrainian officials about this new malware package it has named *"Fox Blade"* (Orenstein, 2022). The Russian Federation has extensive experience in cyber warfare and the Russian cyber infrastructure and equipment have continuously developed in such a way that they have favoured the implementation of hybrid actions. The dynamics of cyber attacks have shown that they are used as a precursor to any form of action, and can continue at a higher intensity or be the opening for a new stage of military operation to achieve their goals. Russia's *modus operandi* was based on experiences from past conflicts with Estonia, Georgia and Ukraine, which came as no surprise to many experts. In the new international context, in which the global security situation is volatile, bellicose statements cause unease and fear even for state actors not directly involved in the conflict.

Amid escalating tensions between the two countries, Russia's military intelligence agency (GRU) launched a series of DDoS attacks against Ukrainian banking, government and defence websites in early February. According to a Microsoft report, two other Russian entities such as the Foreign Intelligence Service (SVR) and the Federal Security Service (FSB) *"conducted destructive attacks, espionage operations, or both, while Russian military forces attacked the country on land, in the air and at sea"* with the aim of *"disrupting or degrading Ukrainian government and military functions and undermining public confidence in the same institutions"* (Orenstein, 2022).

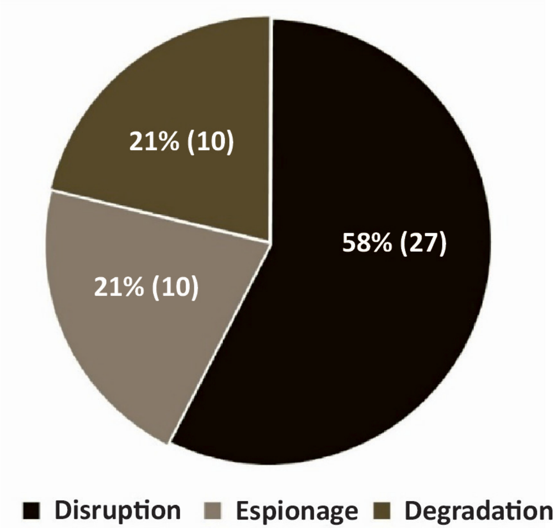

Figure 1: Russian cyber targets
(CSIS, 2023, https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war)

After analysing Russia's cyber activity at the beginning of the conflict, it was found that its cyber objectives focused more on disruptive than degrading actions, which is highlighted in *figure 1*. According to the same sources, Russian cyber activities after 2000 targeted non-state private actors (57%), non-military government actors (32%) and government military actors (11%) (Mueller, Jensen, Valeriano&Mane, 2023). Actions in the cyber environment have become more dangerous with the coordination of conventional military actions in an attempt to create imbalance, panic and confusion among the population. The Russian Federation began preparing for these non-kinetic actions as early as March 2021, while troops were stationed on the border with Ukraine.

Ukrainian government officials reported in January 2022 that, in the first 10 months of 2021, approximately 288,000 cyber attacks were recorded, in addition to the 397,000 attacks recorded in 2020 (Office for Budget Responsibility, 2022). In an interview, Oleksandr Potii, deputy chairman of Ukraine's State Service of Special Communications and Information Protection (SSSCIP), claimed that more than 1,500 cyber attacks against Ukraine were detected in the first six months of the war (Beecroft, 2022). Concurrent with the preparation and conduct of military exercises on the Ukrainian border, these attacks were aimed at gathering foreign policy and military intelligence and gaining access to critical Ukrainian infrastructure. Many of these were launched after various diplomatic talks between the Russian Federation, Ukraine, NATO and the EU failed. Moscow has used these cyber attacks either as a warning or as a threat to make diplomatic actions more serious (Orenstein).

Officials in the Kremlin have said that countries that help Ukraine in this confrontation will face consequences. Indeed, Russian intelligence agencies have stepped up espionage and penetration of communications networks targeting governments sympathetic to Ukraine. Microsoft has detected Russian network intrusion actions against 128 organisations in 42 countries. The top country targeted by these attacks worldwide is the US, while in Europe the priority target has become Poland, Ukraine's neighbouring country that coordinates much of the military and humanitarian logistical support. Russian teams used the Prestige ransomware in this malicious campaign against logistics and transport organisations in Poland, a tactic not commonly used against Ukrainian targets. In addition, the attacks appear to follow a similar pattern to previous hacking activities supported by the Russian Federation (Constantinescu, 2022, p. 23). Other countries that have experienced an increasing number of cyber incidents on computer networks were the Baltic countries, Denmark, Norway, Finland, Sweden and even Turkey.

Particular attention should be paid to Romania, a neighbouring country of Ukraine, on the eastern border of NATO and the EU. It has been the target of such DDoS cyber attacks targeting several institutions, including the Government, the Ministry of National Defence, the Border Police, the Romanian Railways website, banks and other public and private organisations. According to a release from the National Cyber Security Directorate, the websites of these institutions were unavailable for some time and no significant damage was reported (https://dnsc.ro/citeste/comunicat-site-uri-ro-afectate-de-un-atact-de-tip-ddos). Moreover, these incidents were more of a warning and deterrent and were taken over by pro-Russian Killnet hackers. The attacks were motivated by statements of support for Ukraine by leaders in Bucharest, in the context of the invasion of Ukraine by the Russian Federation. Romania was among the first countries to provide humanitarian aid to Ukrainian migrants fleeing the war and has continued to help the neighbouring state in various ways despite the escalation of cyber security incidents.

Briefly analysing Russian actions in the cyber environment, we can make an analogy with the ideas of military theorists starting from Sun Tzu, and continuing with Clausewitz and others who pointed out the need to defeat the enemy even without his physical destruction. Using psychological warfare, disinformation and propaganda spread in the virtual environment, the Russian Federation wanted to shape and incapacitate the essential physical or moral components of the adversary by conquering him without physical combat. Those elements that Clausewitz later called centres of gravity in an adversary were later struck by the Air Force. This Clausewitzian concept of the enemy's centre of gravity lay at the heart of the theories of J.F.C. Fuller, Liddell Hart, John Boyd and John Warden. According to these theories, hitting the centres of gravity could achieve strategic paralysis, thus causing the opponent to give up the fight. Winning the battle was not achieved by physically destroying the fighting forces but by lowering morale through surgical strikes. Moreover, air power had the attribute of striking command and control centres, communications, industrial centres and key elements deep in enemy territory quickly and effectively with maximum efficiency and minimum cost. Therefore, it can be seen that the Russian Federation through its *"cyber paralysis"* aimed at the same effects through its extensive cyber attacks.

On the other hand, the resilience of Ukrainian networks was partly related to actions taken before the conflict to support the development and implementation of a national cyber strategy. Both states have military forces specialising in cyber warfare but have also been supported by patriotic hacker groups who have intervened in support of these institutions either to launch cyber attacks or for cyber defence purposes. In addition, this new way of fighting has attracted the attention of other countries who have readily offered support to these countries, making it an opportunity to test their cyber warfare capabilities for real. Russia's large-scale cyber attacks on Ukraine provide an insight into how it conducts cyber attacks in armed conflict and its hybrid war against the West. More than a year and a half into the war, we can conclude that the Russian Federation is using an amalgam of military techniques and tactics, a combination of the latest tactics and those used in world wars, while also using obsolete weapons simultaneously with sophisticated cyber attacks or attacks using drones, hypersonic missiles or satellite intelligence.

THE IMPACT OF THE RUSSIAN-UKRAINIAN WAR ON CYBER SECURITY IN NATO AND THE EU

It should be stressed that the Russian Federation is vehemently opposed to Ukraine's accession to NATO, as this step would increase Ukraine's military potential and create a regional situation. It is indisputable that the Russian Federation's military aggression against Ukraine has reshaped the threat situation in NATO and the EU, so that the cyber security of the alliances, a component of collective security, has been put to the test. As the conflict has escalated, NATO and non-NATO states have become targets or collateral victims of cyber attacks by Russian state and non-state actors. Moscow has great potential in cyber warfare, and due to its geopolitical situation, it has been successfully adapted to expand its interests. The cyber attacks launched are mostly used in the context of asymmetric conflict (Guchua, Zedelashvili, Giorgadze, 2022, p. 33). According to a Mandiant report, 2022 saw a 250% increase in Russian phishing attempts against Ukraine and a 300% increase in the same attacks against NATO countries (DeCloquement, 2023). All NATO or EU member states that have actively provided political, humanitarian or military support to Ukraine have faced waves of cyber attacks. These operations have been aimed at disrupting national infrastructures, but also at creating a deterrent against intervention in the war. Through social media and attacks on news websites and radio stations, disinformation and fake news, operations were carried out against the Ukrainian government and NATO. The Russians also carried out offensive operations against the US, Poland, the UK, Germany, Latvia, Romania and other countries.

Before the ground invasion began, the Russian Federation deployed malware that disrupted the Viasat satellite system and led to the temporary disruption of more than 30,000 internet connections in Europe, including 5,000 wind turbines. SpaceX claims that the Starlink network has withstood multiple Russian cyber attacks since it was deployed in Ukraine. The European Union has activated its rapid response teams for cyber security incidents to help Ukraine fend off Russian cyber attacks (Mueller, Jensen, Valeriano&Mane, 2023). This new challenge faced by European and NATO states is a new one in which malicious actors aim to degrade critical infrastructure, extract information, steal intellectual property, and disrupt military activities. The Alliance has adopted a comprehensive cyber defence policy and reaffirmed the validity of Article 5 of the North Atlantic Treaty in cyberspace. In addition, the issue of cyberspace has been high on the agenda of heads of state and government at recent summits. Military support for Ukraine is also becoming a European security imperative. Although only NATO can offer Ukraine protection against Russian attacks, member countries failed to agree on a concrete prospect of membership at the July 2023 summit in Lithuania, a sign that no one wants a direct and open confrontation with the Russian Federation. The door to Ukraine's membership of the military alliance remains open, as evidenced by the framework treaty on *"long-term and comprehensive security guarantees"* for Ukraine, to help the country *"defend itself now"*, with bilateral agreements to follow (North Atlantic Treaty Organization, 2023). NATO has gone so far as to accept Ukraine as a contributing participant in the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

In terms of relations with the European Union, Ukraine has been and is considered an important ally. EU leaders have called for the strengthening of cyber threat protection capabilities for both Ukraine and its member states since 2014. Additionally, in 2020, European Commission President Ursula von der Leyen called for greater *"technology sovereignty"*, referencing Asia's technology reliance. Moreover, the EU's dependence on Russian oil and gas has prompted transitional plans to reduce reliance on Russian natural gas and enhance the EU's economic resilience. The economic costs of malicious activities place strain on the resilience of democratic states and institutions, directly threatening the peace and security of the European Union. The focus lies on diplomatic action to support cybersecurity through information sharing and interoperability among member states or between the EU and non-EU states.

In terms of external support, Ukraine has benefited from a substantial increase in cyber support from governments or the services of well-known digital companies such as Microsoft and Amazon. These private companies have far greater analytical capabilities than most Western countries (DeCloquement, 2023).

The Russian-Ukrainian war offers some lessons for future cybersecurity conflicts. Cyber attacks are inevitable and can occur both before and during a conflict. States must be proactive in anticipating these attacks and be prepared to assess, manage, and respond to them quickly. Key partnerships must be established in advance between armed forces, allies, industry, and cybersecurity agencies engaging in proactive defensive cyber operations. These partnerships are a fundamental element in this equation. To be resilient in future conflicts, NATO and EU member states should understand that defensive cyber operations are crucial. Thus, member states' militaries must continue to study Ukraine's past and present experiences to help develop future military capabilities. Moreover, a coordinated and comprehensive strategy is needed to strengthen defences against the full range of destructive cyber operations, espionage, and propaganda. Defensive strategies must take into account the coordination of these cyber operations with kinetic military operations.

Another lesson identified in this conflict is the need to train more cybersecurity incident response teams or utilise artificial intelligence for more effective detection and rapid response to cyber incidents. Additionally, raising awareness among the populations of NATO and EU member states about cybersecurity risks should be done by promoting cyber hygiene to prevent vulnerabilities in information systems, especially during crisis or wartime situations. Furthermore, there is a need to update cyber legislation and invest in innovative technologies to enhance cyber resilience. Drawing from Ukraine's experience, moving data to the cloud has proven to be a solution for more effective data protection. As governments cannot independently develop cyber technologies, software, and expertise, cooperation between public and private services should be fostered in the future, particularly as cyber security firms can aid in cyber defence against large-scale cyber attacks, as witnessed in Ukraine. Moreover, there is a case for increasing interoperability within alliances and beyond by conducting more exercises, crisis simulations, and cyber games to foster a common understanding of the best ways to respond to incidents and mitigate their consequences (Smith, 2022).

The EU Agency for Cybersecurity (ENISA) pays increased attention to cybersecurity in the Common Foreign and Security Policy (CFSP) and promotes cooperation between Member States to implement the Union's cybersecurity policies. Cyberspace can only be effectively defended through strong collaboration. Closer cooperation between NATO and EU cyber initiatives contributes to improving the well-being and security of citizens, protecting critical infrastructure, and strengthening cyber defence. NATO and EU officials recently discussed developments in cyber policy and agreed to continue working closely together to improve common understanding, strengthen cyber capabilities, and prevent, deter, and respond to cyber threats (North Atlantic Treaty Organization, 2023).

At the Vilnius Summit, allies made significant decisions to strengthen cyber defence as part of NATO's overall deterrence and defence strategy. This includes a commitment to strengthen national cyber defences through the Enhanced NATO Cyber Defence Pledge. In addition, the allies launched NATO's new Virtual Cyber Incident Support Capability to support national efforts to mitigate the effects of significant malicious cyber actions. This tool provides Allies with an additional resource for assistance (North Atlantic Treaty Organization, 2023). By managing cyber defence through multilateral structures within NATO, member states can communicate effectively and share experiences to benefit from best practices and collaboration in the effective use of available expertise and resources.

CONCLUSIONS

Under the paradigm of future warfare, cyberspace attacks are likely to be widely used in large-scale operations attempting to bring about the strategic paralysis of the adversary. The use of cyber forces in the future amplifies and enhances the effects of actions in other areas of military operations, a vital element in the multi-domain actions that are increasingly talked about. Cyber actions are used in a complementary or stand-alone manner.

When all advanced systems depend on high-performance sensors, rapid transmission of massive amounts of data, the accuracy of target detection, implementation of targeting, the realisation of satellite communications and development of power projection capabilities through space-based means of surveillance, reconnaissance and communication, all become vulnerable to cyber attacks. However, these systems may not be as vulnerable as any computer network if not secured in time and correctly. The biggest challenge is to succeed in securing command and control systems that can become centres of gravity at different levels of armed combat (strategic, operational, and tactical).

The trend is to move armed combat into cyberspace to reduce the loss of life but to produce the desired political and military effects in a short time and at minimal cost. Responsible authorities can, therefore, provide the answer to adapting the policies governing cyberspace to offensive technological and procedural developments. At the same time, the most valuable resource is people. Educating them on cyber hygiene is an infinite resource, whether they are experts or simple users of digital space. The more educated they are, the better they will know how to identify, dodge, and act promptly to the waves of cyber incidents that the world experiences daily.

This conflict has created an opportunity for the Russian Federation to use cyber attacks in wartime. It also allows analysts to better understand Russia's strategy for cyber attacks. It also provides defence experts with lessons for the future. While no one can predict how long this war will last, the potential for future Russian aggression remains a concern for the European Union and the North Atlantic Alliance.

BIBLIOGRAPHY:

1. Aliyev, N. (24 November 2022). *Riddle*, at https://ridl.io/cyber-operations-during-russia-s-invasion-of-ukraine-in-2022/, retrieved on 12 September 2023.
2. Bateman, J. (2022). *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications.* Carnegie Endowment for International Peace.
3. Beecroft, N. (3 November 2022). *Carnegie*, at https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322, retrieved on 12 September 2023.
4. Constantinescu, V. (11 November 2022). *Bitdefender*, at https://www.bitdefender.co.uk/blog/hotforsecurity/russian-military-threat-group-linked-to-ransomware-attacks-in-ukraine/, retrieved on 22 August 2023.
5. CSIS (2023), https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war, retrieved on 12 August 2023.
6. DeCloquement, F. (27 February 2023). *Cyber-bilan Ukraine*. *Atlantico*. France: Atlantico.
7. Guchua, A., Zedelashvili, T., Giorgadze, G. (2022). *Geopolitics of the Russia-Ukraine War and Russian Cyber Attacks on Ukraine-Georgia and Expected Threats*. *Ukrainian Policymaker*, pp. 27-36.
8. Hakala, J., Melnychuk, J. (2021). *Russia's Strategy in Cyberspace*. Riga: NATO StratCom COE.
9. Herzog, S. (2011). *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*. In *Journal of Strategic Security*, vol. 4, nr. 2, pp. 49-60.
10. Iasiello, E.J. (2017). *Russia's Improved Information Operations: From Georgia to Crimea*. In *The US Army War College Quarterly*, pp. 51-63.
11. Isaacson, W. (7 September 2023). *The Washington Post*, at https://www.washingtonpost.com/opinions/2023/09/07/elon-musk-starlink-ukraine-russia-invasion/, retrieved on 22 September 2023.
12. Lewis, J.A. (2022). *Cyber War and Ukraine.* Washington, D.C: Center for Strategic and International Studies.
13. Michta, A.A. (2015). *NATO's Eastern Front*. In *GLOBAL FORECAST*, pp. 45-47.
14. Mueller, B.G., Jensen, B., Valeriano, B., Mane, C.R. (13 iulie 2023). *Center for Strategic & International Studies*, at https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war, retrieved on 12 August 2023.
15. North Atlantic Treaty Organization. (22 September 2023). *North Atlantic Treaty Organization*, at https://www.nato.int/cps/en/natohq/news_218654.htm, retrieved on 22 September 2023.
16. North Atlantic Treaty Organization. (14 September 2023). *North Atlantic Treaty Organization*, at https://www.nato.int/cps/en/natohq/topics_78170.htm, retrieved on 29 September 2023.
17. North Atlantic Treaty Organization (2023). *Vilnius Summit Communiqué*, at https://www.nato.int/cps/en/natohq/official_texts_217320.htm, retrieved on 22 September 2023.
18. Office for Budget Responsibility. (iulie 2022). *Office for Budget Responsibility,* at https://obr.uk/frs/fiscal-risks-and-sustainability-july-2022/, retrieved on 22 August 2023.
19. Orenstein, M. (7 June 2022). *Foreign Policy Research Institute*, at https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/, retrieved on 22 September 2023.
20. Pinko, E. (22 June 2023). *The Begin-Sadar Center for Strategic Studies*, at https://besacenter.org/the-cyber-domain-in-the-russo-ukrainian-war/, retrieved on 15 September 2023.
21. Salt, A., Sobchuk, M. (2021). *Russian Cyber-Operations in Ukraine and the Implications for NATO*. In *Canadian Global Affairs Institute*, pp. 1-7.
22. Seskuria, N. (2021). *Russia's "Hybrid Aggression" against Georgia: The Use of Local and External Tools.* Center for Strategic and International Studies.
23. Smith, B. (22 June 2022). *Microsoft*, at https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/, retrieved on 22 September 2023.
24. Stanciu, C. (2016). *Viitorul conflictualității – operații asimetrice și hibride.* București: Editura Universității Naționale de Apărare „Carol I".
25. Statista Research Department (16 January 2023). *Statista*, at https://www.statista.com/topics/7335/information-security-and-cyber-crime-in-russia/#topicOverview, retrieved on 21 September 2023.
26. Umbach, F. (16 June 2022). *Reassessing Russia*, at https://www.gisreportsonline.com/r/russia-cyber/, retrieved on 22 August 2023.