ANTE PORTAS

ANTE PORTAS

Security Studies

ISSN 2353 – 6306
December 2024
No. 21

Contact with the Editorial Board
email: redakcja@anteportas.pl

PEER-REVIEWED JOURNAL
Web page: www.anteportas.pl

ISSN 2353-6306

The original version of the journal is the electronic version.
The journal is published as a annual

The journal is indexed in: *Index Copernicus, ERIH Plus, Central European Journal of Social Sciences and Humanities, BazHum, Polska Bibliografia Naukowa*

Cover design: Mateusz Lomber
Technical editing, proofreading and adjustment: Editorial Board

Publisher:

Józef Gołuchowski University of Applied Sciences
Akademicka 12, 27-400 Ostrowiec Świętokrzyski
tel. 041 260-40-41, email: info@goluchowski.edu.pl / redakcja@anteportas.pl

TABLE OF CONTENTS:

II. Reviews

EDITORS' NOTE

As many analysts predicted, 2024 did not bring satisfactory solutions to the stability of the international security architecture. Moreover, it can be said that the situation in the world – In Ukraine, the Middle East and the Far East – is getting more unstable and unpredictable by the month. Many experts put a big question mark on the behavior of one of the most important players on the global geopolitical stage – the United States of America. Without prejudging how U.S. policy will ultimately take shape under the administration of new President Donald Trump, it can already be said without risk that, at least in the declarative sphere, Trump wants to revise many of the strategic policies of outgoing President Joe Biden. In addition, new technological innovations are appearing on the threat map, affecting the functioning of entire societies, but also related to the security sphere. First among these innovations is artificial intelligence.

Many of these issues have become the subject of analysis in this issue of the periodical "Ante Portas - Security Studies". Our authors consider such issues as new security threats, cyber-terrorism, Artificial Intelligence and CBRN, among others. The authors also continue the topic of the Russian-Ukrainian war, not only from a military point of view, but also as an area of financial war or war for food. This issue also includes one review article, by Piotr Gil.

Among the authors were regular editors and contributors to the journal, as well as those who are publishing their texts for the first time in the pages of "Ante Portas - Security Studies". Traditionally, our periodical has gathered an international group of experts – from Poland, Ukraine, Georgia, Moldova, Denmark, the United Kingdom.

Issue 21, as you will have noticed, is reissued as a yearbook. With the release of this issue, we are ending a transitional period in the history of our journal, and in future issues we want to focus on thematic issues, enriched with other materials – reviews, interviews, analysis. Starting in the month of January, the journal will be headed by a new editorial team led by well-known securitologist and political scientist Vakhtang Maisaia.

We wish you enjoyable reading, lots of inspiration, and encourage you to contact our magazine and submit articles and comments.

Wiktor Możgin
Deputy Editor-In-Chief

I. THEMATIC ARTICLES

„Ante Portas – Security Studies”
2024, No. 21
DOI: 10.33674/1202415

Krzysztof SURDYK[1]
Poland

SPACE AS A NEW THEATER OF WARFARE

Abstract: *Objects located in Earth orbits play a huge role in the functioning of our current, terrestrial reality. Disruption or destruction of satellite communication, navigation, and monitoring systems can have catastrophic consequences for the country whose satellites are destroyed. Countries that are leaders in space technology are working intensively to secure their space objects, as well as technologies that allow for the destruction of objects in space. Currently, four countries have the ability to shoot down satellites: the USA, China, Russia, and India. However, none of these countries has a fully developed defense of their satellites. According to experts, a month of combat operations using anti-satellite missiles is enough for both sides of the conflict to be left without orbital satellite groups. The means of destroying satellites are primarily missiles launched from the ground, but also so-called interceptor satellites (fighter satellites, inspection satellites) and other weapon systems placed on orbital platforms. The article presents the importance of space for modern civil and military systems operating on Earth. It indicates the actions of the USA, Russia and China both in the field of defense of their satellite systems and in the area of active offensive actions against the satellite systems of potential opponents. The results of the analysis of the actions of the main competitors in the space arms race lead to the conclusion that a new theater of warfare is being created - the Space Warfare Theater.*

Keywords: *space, satellite, inspection satellite, anti-missile systems, space force, space shuttle, laser weapon*

[1] Krzysztof Surdyk, PhD, Helena Chodkowska University of Technology and Economics (Poland), ORCID: 0009-0002-0654-4095, email: krzysztof.surdyk@interia.pl

Introduction

The issue of transferring potential combat operations to space is not a new idea. As early as 1983, President Ronald Reagan presented the concept of placing innovative types of weapons in space. His Strategic Defense Initiative (SDI), called "star wars", was intended to prevent the USSR from carrying out a retaliatory nuclear strike by effectively eliminating Soviet ballistic missiles using kinetic and energy weapons placed on platforms orbiting the Earth. In the 21st century, plans for the militarization of space began to be developed from the very beginning of its activity in 2001, including the administration of George Bush Jr. They were supported in particular by the head of the Pentagon, Donald Rumsfeld. With the arrival of Donald Trump in the White House (during his first presidential term), discussions about transforming space into a Theater of War (TDW) and saturating the new battlefield with appropriate forces and means began to gain momentum in US political and military circles. The Chief of Staff of the US Air Force, General David Goldfein, spoke in February 2018 about the likelihood of a war breaking out in space within just a few years. He claimed that achieving US superiority in space is as important as maintaining US Air Force superiority in airspace. Many representatives of world expert circles claim that the militarization of space is unavoidable, and claims that the 1967 Space Agreement[2] largely inhibits the processes of transforming space into a new battlefield are simply wrong. Moreover, this agreement only concerns weapons of mass destruction, mainly nuclear weapons, and does not mention other types of weapons at all, such as combat lasers. Even during the Cold War, on the orders of President Reagan, devices for military purposes began to appear outside the Earth's atmosphere. This process is still continuing today.

The importance of space for modern combat operations

Space devices of various types are used, among others, for: conducting satellite reconnaissance, securing communications, naval navigation and land navigation, controlling drones, as well as directing flights of missiles and aerial bombs. Destruction of an orbital enemy group deprives it of satellite

[2] The Outer Space Treaty was signed in 1967 in a situation in which outer space had been governed only by customary law for 10 years, supported by formally non-binding guidelines expressed in the Declaration of Legal Principles of 1963. An important regulation from the point of view of permissible activities in outer space is introduced by Article IV of this Treaty, providing for the partial demilitarization of outer space and the complete demilitarization of celestial bodies. According to it, it is prohibited to introduce into orbit around the Earth any objects carrying nuclear weapons or any other types of weapons of mass destruction.

communication, the ability to conduct reconnaissance from space and use navigation systems. This is a colossal blow to the combat capabilities of modern armed forces. Without satellites, it is impossible to use precision weapons, and the use of aviation becomes more complicated. It is increasingly common to hear the claim that the experience gained from armed conflicts that took place at the end of the 20th and beginning of the 21st century showed that the use of space support systems can be one of the main factors determining victory on the modern battlefield. Thus, it can be observed that the militarization of space is slowly but inexorably entering a new phase. In the initial period of development of military space assets, only "passive" satellites were placed in space, supporting military operations by collecting and transmitting various necessary information. However, today this situation has changed. Tests are being conducted on special unmanned "active" satellites, which, by equipping them with anti-missile systems, are to be able to destroy designated targets. Currently, there is no strict and appropriate definition of space weapons. This leads to a difficult situation related to the unambiguous classification of certain means of destruction. However, it can be assumed that space means of destruction are such means of destruction that are located in space or are intended to destroy objects located there. Thus, we can speak of the following classification of space warfare assets intended to destroy designated targets[3]:

- Earth-to-space assets - placed on the surface of the Earth, and their purpose is to destroy objects located in outer space;
- Space-to-space assets - placed in space, and their purpose is to combat other objects located in near-Earth space;
- Space-to-earth assets - placed in space, and their task is to neutralize targets located on the surface of the Earth.

The greatest hopes for space-based weapons are associated with laser weapons. Work on this type of weapon is being carried out on a very large scale. Currently, there are several types of lasers, such as: free electron lasers, gas-dynamic lasers, X-ray lasers, chemical lasers, and electro-discharge lasers. In addition to laser weapons, large-scale research and development work is also being carried out on particle accelerators (so-called particle weapons), which are designed to destroy objects in space. Research is also being carried out on the creation of kinetic and radiation weapons. All this indicates that in the near future, armed conflicts will be able to take place not only on land, sea and air, but also in space. A huge number of artificial satellites are already orbiting the Earth, one third of which are military devices. In addition, there are thousands of pieces of debris that threaten other objects in orbit. An important role is

[3] B. Watson, B. Peniston, *Space Force moves ahead*, <https://www.defenseone.com/news/2018/07/the-d-brief-july-31-2018/150162/?oref=d-river> (31.07.2018).

played by spacecraft that have the ability to maneuver in orbit to conduct observations or otherwise interact with other satellites. These satellites are called inspection satellites or inspector satellites.

United States

In general, it can be stated that the Pentagon's position in relation to space struggles is as follows: “We must defend ourselves, but we must also be ready to take offensive action to prevent aggression by a potential adversary”. In implementation of this principle, by decision of President Donald Trump, in 2018, a new branch of the military was created in the United States - the Space Forces. These forces supplemented the existing branches of the US armed forces, i.e. land forces, naval forces, air forces, marines and coastal defense. Within the Space Forces, the first to be created are:

- US Space Command, i.e. the 11th combat command;
- Space Operations Forces (the organization of the SOK, similarly to the creation of the US Special Operations Command, involves the relocation and use of space specialists from the entire military);
- Space Development Agency (dealing with all new major satellite programs from now on).

Two key space initiatives are planned for the coming years. It was agreed to work on:

- creating a new system of warning satellites designed to detect ballistic missiles;
- creating weapons systems deployed in space that would destroy these missiles.

Congressmen have adopted a very aggressive schedule for implementing space programs. They want sensors (elements detecting incoming ballistic missiles) to be deployed in orbit as early as 2022. At the same time, the MDA (Missile Defense Agency - MDA) is to begin work on space weapons systems that are to be deployed in orbit by the end of the present decade.

The Americans have been reaching these decisions gradually. As early as 2001, they conducted the first simulation of a space conflict, placing it in 2017, which showed that the United States would suffer such a conflict. They even established the 527th Space Aggressor Squadron, which for now was to only deal with simulations of attacks on military and civilian facilities located in space. In February 2008, a year after the Chinese experiment with destroying a satellite, the Americans conducted their own test. An SM-3 missile from the American cruiser Lake Erie destroyed a US Army reconnaissance satellite (USA-193) filled with poisonous fuel, which had malfunctioned and could have fallen to Earth. It was hit at an altitude of 210 km, when it was moving at a

speed of 27,000 km/h. The experiment showed that a typical defensive system, such as the American “anti-missile shield”, can become a first-strike weapon against objects in orbit. During the Cold War years, the Americans had an orbital group in the so-called “Medium Earth Orbit” - about 20,000 km from the Earth. For many years, these orbits were considered absolutely safe in terms of potential missile attacks. However, in May 2013, the Chinese tested their interceptor missile at an altitude of 30,000. km, which has caused understandable concern in the US and the need to take new steps to protect its satellite groups. In addition to interceptor missiles, the Americans also have other weapons designed to destroy satellites. These include, among others, missiles fired from high-altitude aircraft. Washington is also developing laser weapons that could be used to destroy enemy satellites without the need for missiles. As early as 2001, designers from Lockheed Martin and Boeing conducted successful tests of a laser to neutralize satellites.

A separate issue related to the US military space systems are two very intensively developed programs: “Ballistic Missile Defense” (BMD) and “Prompt Global Strike” (PGS).

According to Russian assessments, both systems were designed as two mutually complementary types of weapons, intended to eliminate Moscow's ability to deliver a nuclear strike on the United States under the principle of "mutual assured destruction". The essence of the PGS is that its weapon systems should destroy the maximum number of Russian ballistic missiles while still in their launch positions. However, those that do manage to launch would be destroyed by the “Anti-Ballistic Missile Shield” anti-missiles. The beginnings of these programs date back to 2002, when the US government withdrew from the 30-year-old ABM Treaty, a ban on anti-ballistic missiles - concluded between the US and the defunct USSR and began to intensively develop anti-missile systems. Currently, the concept of the “Anti-Ballistic Missile Shield” is being implemented - the widely known American multi-layer anti-ballistic defense system, designed as a means against short-range (SRBM), medium-range (MRBM), intermediate-range (IRBM) and long-range (ICBM) ballistic missiles. One of the elements of this system, the SM-3 anti-missile missile base, has just been launched in the Polish town of Redzikowo.

It is worth noting, however, that although the BMD system is of a typically defensive nature, as can be seen from the example of the shooting down of the USA-193 satellite, the “Anti-Missile Shield” anti-missiles can be successfully used not only to destroy ballistic missiles, but also objects in orbit, including satellites or platforms with weapon systems deployed there. Shooting down objects moving along specific ballistic trajectories does not pose a particular problem for specialists. For example, the destroyed American satellite No. 193 flew along a specific orbit, known to the American military. The missile, or rather the SM-3 interceptor anti-missile, was fired towards a previously

calculated rendezvous point and destroyed it with a direct hit[4]. Currently, the Americans are working on modernizing their kinetic means of destruction and are trying to "teach" them to maneuver. In such a case, they will be able to correct the missile's combat mission during its flight. Moreover, as a result of increasing the potential of the low-orbit detection system, data on enemy ballistic missiles, i.e. data on potential targets, will be transmitted to the anti-missile directly from the satellite, correcting its flight.

As for the Prompt Global Strike (PGS) system, there is little published information about it in the United States. Some information can be obtained from statements by Russian experts, who for obvious reasons analyze its potential to harm the Russian strategic missile forces. In recent years, the United States has given absolute priority to the development of the PGS. As part of this program, the Pentagon is creating promising strike systems, and one of the priority weapons systems developed as part of this project is hypersonic missiles (e.g. Falcon HCV)[5]. According to the first deputy head of the operational directorate of the Russian General Staff, Gen. Viktor Poznikhir, the weapons systems developed as part of the PGS are designed to destroy any target within an hour of the decision to attack[6]. Among the systems being developed are those that allow for precise strikes from Earth's orbit on command posts and ballistic missile launchers in Russia. In the conventional (non-nuclear) version, PGS systems are to perform the same tasks that strategic nuclear forces are currently responsible for. According to another Russian military expert, Aleksei Leonkov, the United States has developed several projects for the militarization of space as part of the PGS concept. One of the versions of space weapons developed as part of this concept is the so-called "Rods from God" - a system that operates by "dropping" specially prepared cores made of refractory alloys from orbit onto specific targets on the Earth's surface. In April 2005, together with the first mentions of PGS, information also appeared about plans to build an aircraft orbiting the Earth in the stratosphere and equipped with precisely controlled rockets and bombs weighing half a ton in total. It would be capable of "destroying command centers and missile bases anywhere in the world". Some experts claim that the X-37B mini-shuttle currently being tested not only serves as a spy, but also carries on board weapons systems for destroying satellites, and perhaps even

[4] American (and also Chinese) satellite interceptor missiles operate on the principle of kinetic impact – they destroy the target by colliding with it.

[5] From the speech of the representative of the Ministry of Defence of the Russian Federation Alexander Yemelyanov during the session of the First Committee of the UN General Assembly on 13 October 2017.

[6] General Lance Lord, head of the U.S. Air Force Space Command, delivered a speech to Congress in April 2005.

the aforementioned “Rods of God”, tungsten rods that are to fall from orbit and destroy bunkers hidden deep underground with the force of impact alone.

American military expert John Pike, director of the Globalsecurity.org website, asked directly in the Los Angeles Times: “Are we dealing with a new spacecraft or an orbital bomber?”. Work on the creation of the Boeing X-37 unmanned shuttle, initially known as the flying orbital laboratory, began in 1999. The X-37 was designed to operate at altitudes of 200-750 km, and it can also change orbits and maneuver. Its design allows it to return to Earth just 10-15 days after returning to Earth. could start another expedition. The actual purpose of this orbital aircraft is unknown, although initially, the purpose of its creation was given as the renovation of Earth satellites. It was officially confirmed that the device is testing a new type of ion engine. According to some unofficial information, the X-37 can also perform reconnaissance functions. In the Western media, you can find different versions about the purpose of the development program of this secret, military shuttle. It is said that it can track the Chinese orbital station “Tjangun”, that it can destroy satellites or test technologies related to the deployment of weapons in space in orbit. It is also said that a special chamber has been provided in this device, in which nuclear weapons can be placed.

The problem of protecting satellites, and even entire satellite groups, is absolutely fundamental. According to the commander of the US Space Command, General James Raymond, potential adversaries of the US, namely Russia and China, not only have missiles that can reach American satellites from the ground, but have already introduced systems capable of combating them into Earth orbit. General Raymond claims that in order to “tame space aggressors, the US Air Force is preparing specialized, maneuverable space fighters, the so-called warfighters, whose sole task will be to protect American satellites”. In fact, the discussion in the US about the need to have space fighters with astronauts on board began in 2007, when China tested a ground-based anti-satellite weapon by attacking one of its old satellites at an altitude of about 800 km. The American media suspects that such a warfighter may be the aforementioned X-37B, but John Huten, a senior official from the Space Command, responded negatively to a direct question on this matter. The X-37B program should be replaced soon by the so-called aerospace system program. The American press reported that the first reusable device of this type will fly to the International Space Station. It is obvious that this type of system will also be used for military purposes. According to Russian military experts (Aleksei Leonkov), the aerospace system will pose a significant threat to the Russian system for warning about ballistic missile launches, which will not be able to notice the launch of these aerospace, orbital mini-shuttles. If such a space vehicle is equipped with space-to-earth class rockets, then registering the launch of such a rocket will be practically

impossible. The space control system will identify it as an artificial satellite of the Earth. Currently, experts doubt that the space shuttle (X-37) could be used as a warfighter or orbital bomber. It is too small to accommodate complex weapons systems.

On the other hand, the futuristic rocket plane of the US Armed Forces, XS-1, is presented as an example of an aerospace system. It is to cover several thousand kilometers per hour, brush against space and once a day place a satellite into orbit, which will replace those destroyed by the enemy. The new machine is to be built by Boeing in cooperation with DARPA[7], which is managing the entire undertaking. XS-1 is to be a combination of a launch vehicle and an airplane. In appearance, it will be similar to NASA's space shuttle, although it will not be strictly a space vehicle, because it is not to cross the conventional boundary of the atmosphere at an altitude of one hundred kilometers. It is to take off vertically using a rocket engine, just like a regular rocket, and then turn into an exceptionally fast plane reaching high supersonic speeds - even over 10 thousand km/h. On its back, the XS-1 will carry a smaller rocket with a satellite. When it accelerates sufficiently and gets as close as possible to the edge of space, the rocket will be launched and fly higher, carrying its payload into orbit. After launching the rocket, the vehicle itself will turn around and land like a normal plane - at an airport. It will be ready for the next launch within 24 hours. The main advantage of the XS-1 is to be the ability to perform frequent launches. A maximum of 10 times in 10 days. Americans are very keen on a device that is to be able to launch satellites frequently and quickly. The US armed forces are dependent on numerous communication, navigation and spy satellites. It is assumed that in the event of a major war, satellites will be one of the first targets and at least some of them will be destroyed. Americans are therefore working on a way to quickly replace such losses. The XS-1 is to serve precisely this purpose, not to mention actively influencing the space objects of a potential enemy.

In the context of aerospace systems, it is worth mentioning the pilots who would operate these systems. It is understandable that piloting a warfighter requires special skills and predispositions. It turns out that the preparation of pilots is already being carried out. According to the specialist magazine "Defense Tech", at the "Nellis" Air Force Base (Nevada), at the US Air Force Preparation Center, a program is being carried out to prepare 70 pilots from the 527th Air Force Squadron, which in the future is to protect the orbital grouping

[7] DARPA (Defense Advanced Research Projects Agency) – American government agency dealing with the development of military technology operating within the structures of the U.S. Department of Defense.

of American satellites from missile attacks and electronic warfare (EW)[8]. The general goal of this training program is to obtain appropriate habits by pilots in the scope of responding to any "new and changing threats to space infrastructure objects".

Russian Federation

The Russians have built their own space defense system. The Aerospace Forces of the Russian Federation (Vozdushno-Kosmicheskiye Sily – VKS) began operating in accordance with the decree of the President of the Russian Federation on August 1, 2015, as a new branch of the Russian Armed Forces[9]. The new forces included aviation, air defense and anti-missile defense forces and means, space systems of the so-called "Russian orbital group", and missile attack warning and space control systems. The Russian Space Command (part of the VKS) has three main operational and research centers: the Main Center for Testing, Testing and Control of Space named after G.S. Titov in Krasnoznamensk, the Main Center for Missile Attack Warning (SPRN) in Solnechnogorsk, and the Main Center for Space Surveillance (SKKP) in Noginsky-9, Moscow Oblast. There is no official and reliable data on what specific Russian missiles or other carriers can be used to destroy satellites in orbit. If we talk about modern and promising systems for destroying satellites, then there have been mentions in the press about the use of A-235 "Nudol" anti-missile defense missiles and S-500 "Prometey" anti-aircraft and anti-missile system for this purpose. The A-235 system will have anti-missiles of short, medium and long range in its equipment. Anti-missiles of the earlier A-135 Moscow defense anti-missile system are also being tested. On November 24, at the Sary-Shagan test site in Kazakhstan, as well as on February 12 and April 2, 2018, Russia successfully tested a new version of the PRS-1M anti-

[8] O. Pawlyk, *US Air Force Preparing for War in Space*, <https://www.military.com/daily-news/2017/04/04/us-air-force-preparing-war-space.html> (04.04.2017).

[9] Changes in the airspace command system are a consequence of the integration process that began in the Russian army on July 16, 1997, when a new type of armed forces was created: the Air Force. At that time, the Air Force and the Air Defense Forces were combined under one command. After major structural and organizational changes, the Main Staff and the Command Post of the Commander-in-Chief of the "new" Air Force were finally created. In parallel, work was carried out on integrating all elements related to the use of space and creating management and command system structures - dealing with this area. As a result of these activities, on December 1, 2011, even a new type of armed forces - the "Airspace Defense Forces" - the VKO Troops was created. However, as it turned out, the demarcation of space and air defense systems and aviation is increasingly difficult and many programs must be closely synchronized with each other. Therefore, it was decided to combine everything and thus the Aerospace Forces were created, which joined the other branches of the Armed Forces of the Russian Federation.

missile, which is to replace the PRS-1 (53T6) (Gazelle, according to NATO classification) closer interception anti-missiles in service with the Russian Armed Forces, first tested in 1979. The new anti-missile is to be used in the A-135 “Amur” Moscow defense anti-missile system. With its dimensions preserved, the PRS-1M is in fact a new anti-missile, with a new engine, new electronic equipment, increased flight speed and range. According to preliminary assessments, this new version of the anti-missile is capable of destroying objects in near space. In 2016, 68 shorter-range PRS-1 anti-missiles of the A-135 system were in operation in Moscow's defense. The A-135 system also previously had long-range 51T6 “Azov” anti-missiles (D=670 km, H=70 km), capable of hitting targets in closer space, which were however removed from service due to the expiration of their service life. The original warheads of Russian anti-missiles designed to destroy satellites are equipped with a 10 kT nuclear charge. Unlike the American and Chinese solutions, which use the destruction of satellites in the tests carried out by kinetic impact of the anti-missile on the target, in Russia it is planned to use thermonuclear charges as an anti-satellite weapon. The advantage of this approach is that when such a charge explodes in space, ionizing radiation and a number of other damaging factors destroy not just one satellite, but the entire group of them. This approach does not take into account the enormous damage to the entire planet, but assumes that such a solution will only be used in the event of a nuclear conflict.

In response to the American future aerospace system, which could make it difficult, if not impossible, for the Russians to track American space-to-ground missile launches, Russia has a number of space programs dating back to the Soviet era that have been frozen due to funding constraints. However, if necessary, it can activate them. These programs include the R-36orb missile project, which could strike any point on the globe from space, and the so-called “sputnik hunter” program developed during the Cold War, which supposedly performed a close-in maneuver with a target and hit it with a fragmentation warhead explosion. The first Russian maneuvering device, “Poliot-1”, was launched into orbit in 1963, and the first satellite interception by a satellite was carried out on November 1, 1968. In 1973-76, Moscow sent three Almaz military space stations into orbit. In subsequent years, dozens of tests of interceptor satellites were carried out. The last comprehensive test of the interceptor satellite was carried out in June 1982. This test differed from others in that it was carried out in the conditions of mass launches of ground and sea ballistic missiles, anti-missiles and military satellites. Russians are also working on new systems for combat in space. On April 24, 2017, Pavel Sozinov, the general designer of the Almaz Antey concern, in an interview for the magazine “Национальная оборона” reported that his company, based on the decision of the Russian authorities, had begun implementing the task of

creating a system for countering space-based means. The work involves neutralizing navigational reconnaissance, electro-optical reconnaissance and space-based communication means, as well as direct, physical destruction of these elements moving in orbit.

The Americans claim that the Russians are also conducting secret tests with objects capable of maneuvering in orbit. In 2016, employees of the US Joint Space Operations Center shared with journalists their observations from observing a seemingly routine launch of three Russian communications satellites into orbit. The employees were surprised to find that some small objects identified as fragments of the Russian carrier rocket began maneuvering in orbit. This process lasted several minutes[10]. If we are to believe the bulletin of the American expert-astrophysicist Jonathan McDawell, who conducts observations of various space objects, Russian inspection satellites are also currently conducting maneuvers in orbit. On June 23, 2017, the maneuvering satellite separated from the orbital platform "Kosmos-2519", changed orbit in autonomous flight, then returned to the platform and conducted its inspection. The test tested ground and orbital communication systems, ballistic calculation methods and new satellite software. According to McDawell, the Russian inspection satellite experiment that began in 2017 is still ongoing. Between June 27 and July 19, 2017, the Kosmos-2519 satellite performed a series of engine starts that changed its orbit from 644 x 659 km to 318 x 664 km. Similarly, the Kosmos-2523 satellite performed a maneuver on July 20, 2017 that changed its orbit from 346 x 362 km to 292 x 348 km.

In August 2017, the Russian Defense Ministry confirmed that it had indeed placed a maneuvering inspection satellite into Earth orbit, which had separated from its carrier satellite. It is believed that this satellite is equipped with sensors that allow it to recognize other satellites and transmit the data to Earth for analysis. The Russian Defense Ministry also confirmed the construction of a secret program to build new spy satellites of the Liana system with the Lotos-S and Pion-NKS satellites[11]. It is also expected that the EW system, Buroviestnik-2, which is currently being developed, will be included in electronic warfare with communications satellites. The “Okno” optoelectronic system for detecting space objects, located in the Sangalok Mountains (Pamir) in Tajikistan, at an altitude of 2.2 km above sea level, is also of no small importance to the Russian Aerospace Forces. The system was modernized in 2014 and can now detect any space objects in the altitude range from 2,000 to 40,000 km.

[10] A statement by Lt. Col. Todd Benson of the U.S. Space Command's GPS Division to CBS in 2017.

[11] Based on the statement of Russian Defense Minister Sergei Shoigu from 10.01.2017.

People's Republic of China

The prospects for the development of China's space forces revolve around goals outlined in the early 21st century. One of them is to "gain control of low Earth orbit in order to defeat the United States on Earth". China continues to implement complex satellite maneuvers in Earth orbit, such as: course intersection, conducting operations in close proximity to other satellites. Some of these operations can be viewed as research into dual-purpose technologies with an anti-satellite component. For example, systems for servicing satellites in orbit and technologies for collecting space debris can be used to develop systems for combating satellites[12]. In January 2007, Beijing shot down its own weather satellite Fengyun-1C with a KT-1 anti-missile. This was the first case of a satellite being destroyed by a missile fired from Earth. This sparked strong protests from around the world, the strongest from Washington. Here is another competitor who has gained the ability to conduct warfare in space.

China has been conducting regular tests of interception of extra-atmospheric ballistic targets since 2010. Three years later, Beijing successfully conducted a test of the KT-2 (in Western terminology SC-19) anti-missile to implement such an interception. This system for intercepting orbital targets was given the name Dong Ning-2[13] in China. The Chinese conducted successful tests of this ground-to-space missile (which is an equivalent of the American ballistic missile SM-3), designed to destroy communication satellites, but is also capable of destroying a spy satellite flying at an altitude of 247 km.

For five years, the remotely controlled Chinese inspection satellite Shiyan-7 has been placed in orbit, which has a system for detecting weapons in satellites belonging to other countries. Some experts believe that it is also adapted to destroy such satellites. The consistency in achieving China's goals is also evidenced by the tests of the DF-ZF hypersonic glide vehicle conducted in 2015. It reaches speeds of Mach 5 to 10 and is capable of carrying a nuclear warhead[14].

China has also formed units and is already conducting initial exercises of its anti-space capabilities, directed against the anti-satellite ground-based missile systems of a potential adversary. Similar systems are also likely to be developed in Russia. Both countries are also developing directed energy systems that can "blind" or damage sensitive optical sensors of satellites, such as satellite sensors warning of missile attacks". The possibilities of China's

[12] From the report of the Director of National Intelligence D. Coats to Congress on May 10, 2017.

[13] A. Rezchikov, M. Voronova, Kitay sumel priblizit'sya k protivoraketnym vozmozhnostyam Rossii i SSHA, gazeta VZGLYAD, 6 fevralya 2018.

[14] P. Łepkowski, *Militaryzacja kosmosu: Powrót do gwiezdnych wojen*, <https://www.rp.pl/kosmos/art2049101-militaryzacja-kosmosu-powrot-do-gwiezdnych-wojen> (22.03.2018).

(and Russia's) actions in space were discussed by the head of US National Intelligence, D. Coats, who stated that "Russia and China are developing anti-satellite weapons systems that will reach combat readiness within the next few years". Among the weapons systems being developed in these countries, D. Coats mentions, among others, missile systems and laser weapons.

Summary

The current activities of the US administration and Congress related to the organization of the Space Force and military programs in space are basically the sanctioning and ordering of activities that were actually conducted earlier by the United States. They are also an expression of American assessments of the activities of their main competitors in space. According to the May 2017 report by the Director of National Intelligence, Daniel Coats, the reforms of the armed forces conducted in China and Russia in recent years indicate that these countries are increasingly focusing on creating operational forces that will integrate attacks against American space systems and the functions performed with their help. The Americans are aware that if a war with a serious adversary broke out, their satellite systems would be attacked in the first minutes of the conflict. According to Coats, "Russia and China are developing a whole range of anti-satellite weapons as a means of limiting the effectiveness of the US armed forces, although publicly and at the diplomatic level they will strive for the demilitarization of space and talk about the principle of not deploying weapons in space, first". According to the forecasts of a special commission of the US Congress, China will obtain a full anti-satellite arsenal within the next five years. The Americans intend to use this time to create new radar systems (their production has already begun), which will allow for an anti-missile maneuver or the destruction of a Chinese anti-missile by a space fighter (warfighter). However, if lasers are used to destroy American satellites, the situation will become dangerous for the Americans. In such a situation, no warfighter with astronauts on board will help.

In Russia, Trump's decision to create the Space Forces was received with great concern. The chairman of the Federation Council's Committee on Defense and Security, Viktor Bondarev, stated in a statement for RIA Novosti that "if the United States violates the treaty banning nuclear weapons in outer space during the creation of the Space Forces, Russia will resolutely resist the United States". According to him, the militarization of space is a path to disaster. He emphasized that "if the United States withdraws from the 1967 agreement banning nuclear weapons in outer space, there will be a decisive reaction from Russia, as well as from other countries possessing such weapons". American initiatives related to space, and primarily the Prompt Global Strike (PGS) program, have been and are being very closely monitored in Moscow. This is

evidenced by the statements of many Russian politicians and experts, including Russian Deputy Prime Minister Dmitry Rogozin (from 17.03.2018), who stated that "all current concepts held by the US and its allies assume the possibility of an immediate global strike against Russia using space".

There are also opinions in Russia that Washington's recent steps are intended to force Moscow to increase its defense spending to a level that would cause it serious economic problems, i.e. lead to a situation in which the USSR found itself in 1989. However, awareness of this situation is rather widespread among Russian decision-makers. According to military experts, "Russia will not repeat the mistakes of the USSR and will develop hypersonic weapons systems, the models of which it already has, and whose potential allows it to eliminate the capabilities of hypothetical space interceptors of the US". Observing the events of recent years related to the activities of world powers in space, it can be stated that both the USA, Russia and China are conducting scientific research and testing of reconnaissance systems and space weapons systems, which in the near future may become indispensable components of the armed forces of these countries. The following picture emerges from the analysis of these activities.

The United States, many years ago, developed concepts of operations in space that would allow them to gain a strategic advantage over their competitors, especially over Russia. These include, among others, the BMD and PGS programs described above, programs to deploy particle and laser weapons in space, etc. For many years, the United States has used pretexts to create these systems, such as Iran's and North Korea's nuclear weapons and ballistic missiles. However, the time has come to "drop the visor" and show that their main opponents in space are Russia and China. Hence the decision to create the US Space Force, as well as the official call from Congress for the actual militarization of space (placing sensor and weapon platform groups in orbit). It is also clear that the Americans are taking the organization of their forces in space seriously and comprehensively. Hence the long-term implementation of the BMD and PGS programs, independent of the host in the White House, as well as projects related to the protection of satellite groups (aerospace system). China is consistently implementing its plan to use space for military purposes, although it distances itself from accusations related to the desire to militarize space. In relation to the United States, it has a lot to catch up on, but the country's significant financial capabilities, the first achievements in offensive actions against objects in orbit presented above, as well as the many space science programs that it is implementing, testify to its great capabilities in this area. Russia, declaratively, is currently not interested in militarizing space. This is due to several reasons, including a limited budget and awareness of the risks associated with the implementation of American programs (mainly PGS and BMD). However, it has extensive experience in implementing space programs, gained from the Soviet era, which it is now trying to use. Due to

limited possibilities of financing expensive space projects, Moscow is not able to join the arms race in space and will certainly not repeat the mistake that the Soviet leaders made in connection with Ronald Reagan's SDI program. Instead, it is looking for cheaper alternative solutions that would allow its satellites and ballistic missiles to avoid destruction, for example, by American anti-missiles. Hence the tests of maneuvering satellites in orbit, the introduction of new ballistic missile systems whose warheads can maneuver on different flight sections (RS-24 Jars, Oresznik on the base of RS-26 Rubież), as well as the introduction of hypersonic weapon systems (Avangard), which after entering space reach speeds of 27 M, re-enter the Earth's atmosphere and maneuver towards the target.

In summary, we can say that a change in the approach to the issue of military use of space is taking place before our eyes. The previous acceptance of the use of military satellites for reconnaissance, navigation and communication purposes is beginning to be expanded to include additional functionalities, and attempts related to maneuvering satellites in orbit are not questioned by anyone. Aerospace units are being created and trained (we know about those in the USA). We can therefore say that a new space theater of warfare is emerging before our eyes. Assuming that the transfer of certain weapons systems to space is basically inevitable, we should hope that politicians and military will have enough imagination not to place weapons of mass destruction in space, and above all nuclear weapons.

BIBLIOGRAPHY:

1. Dura M., *Rosja sformowała wojska powietrzno-kosmiczne. Nowy rodzaj sił zbrojnych*, <https://www.defence24.pl/rosja-sformowala-wojska-powietrzno-kosmiczne-nowy-rodzaj-sil-zbrojnych>
2. Gur'yanov S., Genshtab: SSHA poluchat oruzhiye dlya mgnovennogo global'nogo udara v 2020 godu, <vz.ru›news/2017/4/26/867987.html>
3. Ivanov B., Teatr voyennykh deystviy ukhodit na orbitu, <http://nvo.ng.ru/realty/2018-06-29/1_1002_tramp.html>
4. Kanawka K., *Układ kosmiczny – fundament reżimu prawnego przestrzeni kosmicznej*, serwis Kosmonauta.net
5. Kaczorek Ł., *Militarne wykorzystanie przestrzeni kosmicznej*, <http://lukaszkaczorek.blogspot.com/2014/01/militarne-wykorzystanie-przestrzeni.html>
6. Łepkowski P., *Militaryzacja kosmosu: Powrót do gwiezdnych wojen*, <https://www.rp.pl/Kosmos/180329705-Militaryzacja-kosmosu-Powrot-do-gwiezdnych-wojen.html>

7. Pawlyk O., *US Air Force Preparing for War in Space*, <https://www.military.com/daily-news/2017/04/04/us-air-force-preparing-war-space.html>
8. *Projekt XS-1. Amerykański robot do prowadzenia wojny w kosmosie*, TVN24, May 26, 2017, <http://www.tvn24.pl>
9. Rezchikov A., Voronova M., Kitay sumel priblizit'sya k protivoraketnym vozmozhnostyam Rossii i SSHA, gazeta VZGLYAD, 6 fevralya 2018Trevithick J., *Congress Demands Space-Based Missile Defense Weapons and Sensors no Matter What*, <http://www.thedrive.com/the-war-zone/22380/congress-demands-space-based-missile-defense-weapons-and-sensors-no-matter-what>
10. Watson B., Peniston B., *Space Force moves ahead*, <https://www.defenseone.com/news/2018/07/the-d-brief-july-31-2018/150162/?oref=d-river>
11. Weisgerber M., *Space Force moves ahead*, <https://www.defenseone.com/news/2018/07/the-d-brief-july-31-2018/150162/?oref=d-river>

„Ante Portas – Security Studies”
2024, No. 21
DOI: 10.33674/1202416

Levan KALATOZISHVILI[1]
Georgia

THE INTERSECTION OF AI, CYBERTERRORISM AND HYBRID WARFARE: A NEW PARADIGM IN GLOBAL SECURITY

Abstract: *This article explores the relationship between cyberterrorism, artificial intelligence (AI), and hybrid warfare, with a particular emphasis on how AI-driven technologies are changing how modern combat is conducted. The study looks at how AI strengthens cyberterrorism's capabilities and combines with more general hybrid warfare strategies to increase its influence on international security. An extensive case study of the conflict between Russia and Ukraine shows how AI-enhanced cyber operations target vital infrastructure and sway public opinion. The paper also discusses the inadequacies in the present international legal frameworks governing AI in conflict, as well as the ethical issues, such as civilian injury and responsibility in autonomous systems. The paper's conclusion offers strategic recommendations for thwarting these new dangers through enhanced AI defenses and global collaboration.*

Keywords: *cyberterrorism, Artificial Intelligence, hybrid warfare, global security, AI ethics, Russia-Ukraine war*

Introduction

Background

Modern warfare is characterized by sophisticated techniques based on hybrid warfare, which combines cyber operations with military tactics and media campaigns, making it unique and complex in comparison to conventional

[1] Levan Kalatozishvili, MA, Caucasus International University (Georgia), email: levan.kalatozishvili@ciu.edu.ge

methods. Non-conventional warfare was differentiated by its novelty, as opposed to conventional means, which grew even more unique by merging cyber and information operations. Hybrid warfare has merged many types of combat, making it more complex and producing confusing threat environments[2]. This strategy enables state and non-state actors to exploit an adversary's weaknesses for both physical and non-physical effects. These approaches blurred the boundary between war and peace.

In the context of hybrid warfare, cyber operations have emerged as an extremely important mechanism through which actors can conduct intelligence operations, threaten critical infrastructure, and manipulate mass information through access. Cyber-attacks can be launched from anywhere in the world, making them a useful tool for asymmetric warfare[3]. The goal of these operations is to create more vulnerabilities for the adversary without overt military intervention, focusing on creating chaos, vulnerability, and trust in society, mostly involving non-military critical infrastructure.

Hybrid warfare has been taken to a new level by artificial intelligence, which plays an important role in enhancing the effectiveness of cyber capabilities[4]. Massive volumes of data may be processed by artificial intelligence, which then creates algorithms to identify vulnerabilities, anticipate potential targets, and instantly adjust to existing tactics, making cyberattacks more sophisticated and difficult to defend against.

The development of artificial consciousness abilities in digital and data fighting has created new challenges for worldwide security. The consolidation of artificial reasoning into these cycles not only builds the variety and intricacy of dangers, but it additionally recoils the contention line by permitting assaults to be completed quicker, cautiously, and more resoundingly[5].

Research Question

The incorporation of artificial brainpower (computer-based intelligence) into cyberterrorism is changing the essence of present-day battle, especially half-breed fighting. As computer-based intelligence-fueled advances become further

[2] L. Dorosh, O. Ivasechko, J. Turchyn, *Comparative Analysis of the Hybrid Tactics Application by the Russian Federation in Conflicts with Georgia and Ukraine*, „Central European Journal of International and Security Studies" 2019; Vol. 13, Issue 2, pp. 48-73.

[3] W. Wróblewski, *Terrorism and the Hybrid Warfare in Aspect of War in Ukraine*, „Polish Political Science Yearbook" 2022, Vol. 51, Issue 4, pp. 95-107.

[4] J. Johnson, *The AI Commander Problem: Ethical, Political, and Psychological Dilemmas of Human-Machine Interactions in AI-enabled Warfare*, "Journal of Military Ethics" 2022, Vol. 21, Issues 3-4, pp. 246–271.

[5] I. Szabadföldi, *Artificial Intelligence in Military Application – Opportunities and Challenges*, „Land Forces Academy Review" 2021, Vol. 26, Issue 2, pp. 157-165.

developed and available, their utilization in cyberterrorism procedures raises serious worries about their effect on half-breed fighting strategies and viability.

This research seeks to explore and answer the central question: How does the consolidation of artificial reasoning into cyberterrorism influence crossover fighting techniques and viability?

To resolve this issue, the paper features a couple of vital places:

1. Key Advancement: How AI improves state and non-state actors' strategic capacities to carry out hybrid warfare, especially in the fields of information warfare and cyber operations.
2. Operational Effectiveness: The degree to which hybrid warfare methods become more impactful, accurate, and efficient as a result of AI-driven cyberterrorism[6].
3. Global Security Implications: The wider effects of AI-enhanced cyberterrorism on global stability, such as the possibility of further conflicts, the decline in confidence in digital infrastructure, and the difficulties in identifying and countering these sophisticated threats[7].
4. Case Studies and Examples: In order to comprehend how AI-driven cyber operations have been used in hybrid warfare, real-world situations like the Russia-Ukraine conflict will be examined. This will provide insights into the usefulness and practicality of these tactics[8].

By means of this investigation, the study seeks to illuminate the revolutionary function of artificial intelligence in contemporary warfare, providing a thorough grasp of its influence on the mechanics of hybrid warfare and the new threats it poses to international security.

Importance

The combination of cyberterrorism, artificial intelligence (AI), and hybrid warfare is transforming the global security landscape. Complex and multi-layered risks emerge as these elements come together, challenging established safety systems and crucial standards. Understanding the assembly is crucial in view of various considerations:

1. Escalating Threat Complexity: The combination of AI with cyberterrorism in hybrid warfare greatly expands the range and

[6] P. Sharma, K. Sarma, N. Mastorakis, *Artificial Intelligence Aided Electronic Warfare Systems-Recent Trends and Evolving Applications*, „IEEE Access" 2020, Vol. 8, pp. 224761-224780.

[7] O. Ronzhes, *The role of digital technologies in the adaptation of citizens of Ukraine to military aggression by the Russian Federation*, „Scientific Studios on Social and Political Psychology" 2022, Vol. 28, No. 2.

[8] L. Dorosh, O. Ivasechko, J. Turchyn, *op. cit.*

complexity of threats. These cutting-edge dangers have the capacity to compromise public safety, damage vital systems, and alter information.

2. Global Security Implications: AI-powered cyberterrorism, as part of hybrid warfare, may carry out stealthy, quick, and devastating operations, reducing the threshold for conflict. This raises the possibility of unanticipated, difficult-to-identify disputes that might destabilize international relations.
3. Strategic and Strategy Challenges: Traditional defense systems may struggle to combat AI-driven cyber operations in hybrid warfare. Creating new structures and laws is necessary to properly address these developing challenges.
4. Ethical and Legal Considerations: Significant ethical and legal concerns are brought up by the use of AI in cyberterrorism and hybrid warfare, including the targeting of civilian populations and the funding of disinformation campaigns. Legislators must handle these issues within the bounds of the current moral and legal systems.
5. Future Security Preparedness: Anticipating potential hazards becomes increasingly important as AI technologies continue to advance. Comprehending the present and possible consequences of this convergence enables politicians, military strategists, and security specialists to formulate preemptive plans and institute flexible defensive systems.

In conclusion, comprehending how AI, cyberterrorism, and hybrid warfare intersect is not just a necessary intellectual endeavor but also a vital one for maintaining both present-day and long-term international security. In an increasingly digitized and linked world, it provides stakeholders with the information they need to confront the serious problems these interlinked dangers offer, assisting in preserving international stability.

Understanding Hybrid Warfare

Definition and Components

Cross-breed fighting is an essential way to deal with the struggle that consolidates customary military strategies with unpredictable ways to deal with establishing a diverse and dangerous climate. Dissimilar to conventional fighting, which depends on immediate, clear military activity, crossover fighting utilizes military, digital, data, and other irregular methods to accomplish key goals. This strategy empowers state and non-state entertainers to take advantage of the whole range of fighting, utilizing various instruments and methodologies to undermine, disturb, upset, and debase enemy capacities without the requirement for an open clash.

The main components of hybrid warfare are: Ordinary military strategies involve the utilization of normal military, for example, land powers, flying corps, and naval forces, in direct battle tasks. Be that as it may, in half-and-half fighting, ordinary soldiers are often joined with other, less obvious strategies, making it harder for the objective country to successfully answer[9].

Digital Tasks: Digital activities have an important role in crossover combat, empowering surveillance, harm, and disruption of the fundamental structure. Digital assaults can target a country's monetary frameworks, power matrices, exchange organizations, and government data sets, producing significant damage with minimal physical presence[10].

Data Fighting: Data fighting is the use of propaganda, deception, and mental activity to influence general opinion, foment friction, and undermine trust in organizations. This might involve controlling media outlets, internet entertainment, and other avenues of communication in order to spread rumors and stir up trouble.

Unusual techniques include close-quarters warfare, mutiny, and the use of intermediary authorities to repel attacks and destroy districts. Flighty techniques are widely employed to create ambiguity and potential deniability, making it difficult for the target country to identify the true source of the threat.

Money-related and political strain: Mix battling habitually incorporates monetary assent, political threatening, and different sorts of fragile abilities to debilitate the adversary. These demonstrations can hurt the nation's economy, influence political choices, and subvert public confidence in government associations[11].

Mix fighting is supposed to take advantage of a foe's deficiencies by combining these parts in an organized, synchronized way. The object is to accomplish basic objectives through furious, no-limits contests, making it an especially powerful device in the present worldwide scene.

The Role of Cyber Operations in Hybrid Warfare

Today, cyber operations are an essential component of hybrid warfare, boosting the impact of each symmetrical and asymmetrical actions. In hybrid warfare, cyber operations are employed to disrupt activities, reducing the opponent's capacity to respond appropriately to military and non-military threats. Disruption or destruction to essential infrastructure, communication

[9] L. Herța, *Hybrid Warfare – A Form of Asymmetric Conflict*, Sciendo: International conference KNOWLEDGE-BASED ORGANIZATION 2017, Vol. 23, Issue , pp. 135-143.
[10] O. Ronzhes, *op. cit.*
[11] L. Dorosh, O. Ivasechko, J. Turchyn, *op. cit.*

networks, and information systems can destabilise a country, erode public trust, and create favourable conditions for the aggressor.

Key roles of cyber operations in hybrid warfare include:

1. Infrastructure Disruption: Cyberattacks have the potential to completely destroy vital infrastructure, including communication networks, water supply systems, and power grids, resulting in severe chaos and disruption.
2. Surveillance and Intelligence Gathering: By obtaining intelligence on an adversary's military prowess, political schemes, and economic weaknesses, cyber operations provide attackers with a tactical edge.
3. Psychological and Information Warfare: Cyber operations facilitate the dissemination of propaganda and misinformation, influencing public opinion, dividing communities, and eroding confidence in governmental institutions.
4. Economic Disruption: Cyberattacks can damage a nation's overall resilience by focusing on financial institutions like banks and stock exchanges, which can lead to economic instability[12].
5. Covert and Deniable Attacks: The capacity to launch stealthy and defensible strikes is one advantage of cyber operations in hybrid warfare. The reaction might be complicated since these activities can be carried out covertly, making it difficult for the targeted nation to identify the attacker.

Recent occurrences, like the conflict between Russia and Ukraine, have shown how strategically important cyber operations are to hybrid warfare. Cyberattacks have been essential in undermining Ukraine's resistance since they have been used to compromise the country's infrastructure, disseminate false information, and get intelligence. Cyber capabilities will probably play a bigger part in hybrid warfare as they develop, thus it will be more crucial than ever for countries to have strong defenses and counterstrategies.

The Rise of AI in Cyberterrorism

Definition and Scope of Cyberterrorism

Cyberterrorism is the use of digital assaults by people, organizations, or nations to further political, ideological, or geopolitical objectives by causing a great deal of disruption, fear, or harm. Cyberterrorism uses the internet and other digital technology to further its objectives, in contrast to conventional terrorism, which frequently entails physical violence. Critical infrastructure, including power grids, water supply systems, transportation networks, financial

[12] O. Ronzhes, *op. cit.*

institutions, and communication networks, as well as a country's overall social stability, are frequently the main targets of cyberterrorism.

The objectives of cyberterrorism can vary widely but typically include:

- Disruption of Critical Infrastructure: Cyberterrorists seek to disrupt key services, resulting in widespread disruption, economic loss, and human misery. By focusing on essential systems, they can have ripple effects that disrupt daily life and undermine public trust in the government's capacity to safeguard its population.
- Economic Damage: Attacks against financial systems, such as banks, stock exchanges, and internet payment networks, can cause widespread economic turmoil. The consequent financial losses can erode investor confidence, disrupt markets, and harm a country's economy[13].
- Psychological Impact: The primary purpose of cyberterrorism is to generate fear and uncertainty in the people. High-profile attacks that receive significant media attention can compound their impact, spreading dread well beyond the immediate consequences of the attack[14].
- Political and Ideological Influence: By interfering with government operations, influencing elections, or disseminating propaganda, cyberterrorism can further certain political or ideological objectives. Cyberterrorists can attack public communication platforms, government websites, or election systems in an effort to erode governmental authority and threaten democratic processes[15].

Because it is difficult to identify, pinpoint, and combat, cyberterrorism represents a serious danger to both national and international security. These issues have been made worse by the emergence of cutting-edge technology like artificial intelligence, which has increased the sophistication and danger of cyberterrorism.

AI's Role in Enhancing Cyberterrorism

Artificial intelligence (AI) has arisen as an extraordinary power in the field of cyberterrorism, improving the capacities of assailants in a few key regions. The incorporation of simulated intelligence into cyberterrorism tasks empowers

[13] Y. Pachankis, *Technical analysis on the cyber organizational criminology of dictatorial military conducts – experience from human trafficking and coercions by military cyber aggressions*, „International Journal of Security Privacy and Trust Management" 2022, Vol. 11, No. 3, pp. 1-19.

[14] A. Beccaro, *Modern Irregular Warfare: The ISIS Case Study*, „Small Wars & Insurgencies" 2018, Vol. 29, Issue 2, pp. 207-228.

[15] W. Wróblewski, *op. cit*.

more modern, proficient, and significant assaults, introducing new difficulties for online protection experts and state run administrations around the world.

Key ways in which AI enhances cyberterrorism include:

1. Automated Attacks: AI makes complicated hacks automated and scalable, allowing for several simultaneous strikes with little to no human intervention.
2. Target Selection: Artificial intelligence uses massive data analysis to identify the most valuable and susceptible targets for more potent attacks.
3. Evasion Techniques: Real-time adaptation of attack patterns by AI makes it more difficult for security systems to identify and block.
4. Deepfakes & Disinformation: Artificial intelligence produces lifelike false material to propagate misinformation, sway public opinion, and incite social upheaval.
5. Adaptive Malware: Malware and ransomware powered by AI grow more tenacious, adapting and learning to avoid detection and maximize harm.

Potential and Observed Use Cases in Recent Global Conflicts:

1. Russia-Ukraine Conflict: Cyberattacks powered by AI have attacked Ukrainian infrastructure, interfering with military activities and disseminating false information to reduce the country's resilience.
2. Election Interference: Election integrity has been compromised by the use of AI in cyberterrorism efforts to create deepfake material and automate misinformation.
3. Critical Infrastructure Attacks: Power grids, financial institutions, and healthcare systems have all been the target of AI-enhanced assaults, revealing the potential for substantial disruption and financial loss.

As AI technology based intelligence innovation keeps on advancing, its job in cyberterrorism is probably going to extend, making it progressively significant for state run administrations and network protection experts to foster high level safeguards that can stay up with these arising dangers. The ascent of artificial intelligence in cyberterrorism highlights the requirement for an exhaustive and proactive way to deal with network safety, one that expects what's to come difficulties presented by these strong and developing advances.

The Convergence of AI, Cyberterrorism, and Hybrid Warfare

Strategic Integration

The union of artificial consciousness (computer based intelligence), cyberterrorism, and crossover fighting addresses a critical development in the essential scene of present day struggle. This mix permits both state and non-

state entertainers to direct more refined and composed activities, mixing artificial intelligence upgraded cyberterrorism with customary and capricious fighting strategies. This essential incorporation is reshaping the idea of contention by empowering a more consistent and productive execution of crossover fighting, where digital and artificial intelligence innovations assume a focal part.

1. AI-Enhanced Cyberterrorism in Hybrid Warfare: The consolidation of simulated intelligence into cyberterrorism considers more exact, robotized, and adaptable assaults that can be synchronized with different components of cross breed fighting[16]. For example, simulated intelligence can be utilized to disturb correspondence organizations, debilitate basic foundation, and spread disinformation, all while regular military powers participate in actual activities. This organized methodology can make a diverse danger that overpowers the objective's capacity to really answer.
2. State and Non-State Actors Leveraging AI**:** Both state and non-state entertainers are progressively perceiving the worth of simulated intelligence in improving their cross breed fighting capacities.
   - State Actors: Legislatures can utilize simulated intelligence driven digital activities to debilitate foes without falling back on direct military showdown. For instance, simulated intelligence can be utilized to direct digital surveillance, harm basic framework, and control public insight through data fighting. These strategies can accomplish vital goals while keeping up with conceivable deniability, making it challenging for the objective to answer without raising the contention.
   - Non-State Actors: Psychological oppressor associations, radical gatherings, and other non-state entertainers can likewise use simulated intelligence to upgrade their cyberterrorism capacities as a component of a more extensive mixture fighting technique. Artificial intelligence can empower these gatherings to lead more compelling and expansive assaults, permitting them to challenge state entertainers and seek after their philosophical or political objectives with more prominent effect[17].

[16] K. Hanratty, *Artificial (military) intelligence: enabling decision dominance through machine learning*, „Defense + Commercial Sensing" 2023, Vol. 12538.
[17] M. Petrosyan, *The Role of Non-State Actors in Modern Warfare: The Case of Syria and Nagorno-Karabakh*, „Journal of Balkan and Near Eastern Studies" 2023, Vol. 26, Issue 2, pp. 149-163.

Examples

Russia-Ukraine Conflict: In the Russia-Ukraine war, AI driven digital tasks have been coordinated into the more extensive technique of half and half fighting. Cyberattacks have designated Ukrainian foundation, upset military correspondences, and spread disinformation to debilitate Ukrainian obstruction and sow disarray. These activities have been supplemented by customary military strategies, showing the essential combination of simulated intelligence upgraded cyberterrorism inside mixture fighting.

Election Interference Campaign: State entertainers have utilized artificial intelligence to lead digital activities pointed toward affecting races in different nations. These tasks frequently include a mix of digital undercover work, disinformation, and the making of deepfake content, all intended to disturb vote based processes and accomplish vital goals without direct military mediation.

Impact on Global Security

The combination of cyberterrorism, AI, and hybrid warfare has a profound effect on global security by obfuscating conventional military lines and making conflicts more complicated.

Increased Unpredictability: Rapid, covert, and massive attacks are brought about by AI-driven operations in hybrid warfare, making it difficult for targeted governments to foresee and neutralize threats. Because AI can adapt, there is a greater chance of unexpected conflict escalation.

Blurring of Traditional Warfare Boundaries: International conventions and engagement guidelines are complicated by hybrid warfare, which blurs the boundaries between military and civilian targets, conventional and unconventional tactics, and war and peace through the use of AI and cyberterrorism.

Lowering the Threshold for Conflict: AI-enhanced cyber operations may be covert and inexpensive, which encourages actors to participate in conflicts without fear of instant reprisal. This might result in an increase in the frequency of low-intensity conflicts that have the potential to grow.

Challenges for Global Security Governance: Due to the fact that existing international rules are frequently insufficient to meet cyber dangers improved by AI, the merger of AI and cyberterrorism poses serious issues for global security governance. This legal void undermines international stability and makes diplomacy more difficult.

Potential Outcomes

Erosion of Trust in International Institutions**:** Global governance may be undermined by the growth of AI-driven cyber operations, which might erode

confidence in international organizations and agreements and encourage more unilateral action rather than collaboration.

Arms Race in AI and Cyber Capabilities**:** An arms race in cyber and AI technologies might be sparked by the increasing use of AI in hybrid warfare, as nations vie to create cutting-edge offensive and defensive systems. This rivalry might further undermine international security since it is accelerating efforts to set norms.

Final Analysis**:** International security is seriously threatened by the confluence of AI, cyberterrorism, and hybrid warfare. This threat is real and growing. In an increasingly digital world, the international community has to create new frameworks, tools, and tactics to tackle these intricate problems and protect world stability.

Case Study: The Russia-Ukraine War

The Russia-Ukraine War as an Example of AI-Driven Hybrid Warfare

A clear and compelling illustration of how AI-driven hybrid warfare is changing contemporary conflict is the Russia-Ukraine war[18]. Within the larger context of hybrid warfare, this war has brought attention to the expanding role of AI-enhanced cyberterrorism. It has also shown how these technologies can be strategically combined to achieve military and political goals with potentially disastrous effects on international security.

Intersection of AI, Cyberterrorism, and Hybrid Warfare: AI is now being tested in conjunction with cyberterrorism and hybrid warfare strategies in the Russia-Ukraine conflict. Russia's strategy has combined information warfare, hacking, conventional military operations, and political manoeuvring in a sophisticated way, all enhanced by artificial intelligence technologies. Due to this convergence, Russia is now able to carry out a complex campaign that simultaneously affects public opinion and perceptions abroad and targets Ukraine's digital and physical infrastructure.

Specific Examples of AI-Enhanced Cyber Operations:

- Targeting Critical Infrastructure**:** Artificial intelligence (AI)-driven cyber operations have been used to interfere with Ukraine's vital infrastructure, like as its electricity and communication networks and financial systems, throughout the conflict. For example, the notorious hack on Ukraine's power grid in 2015 set the stage for more advanced AI-enhanced attacks even though it happened before the full-scale invasion. The goal of these activities has been to severely impair

[18] W. Wróblewski, *op. cit*.

Ukraine's capacity to maintain vital services and its defense, which will reduce the nation's overall resilience.

- Disruption of Communications: AI has been a major factor in the disruption of military and civilian communications in Ukraine. Automated phishing tactics and malware powered by artificial intelligence have been used to breach communication channels, capture private data, and disseminate false information. These actions are intended to cause disarray and interfere with coordination among Ukrainian forces, making it more difficult for them to effectively counter Russian military advances.
- Influencing Public Perception**:** AI has also proved crucial to the information warfare aspect of the conflict between Russia and Ukraine. Artificial intelligence (AI) algorithms have been used to boost misinformation operations on social media, fabricating and disseminating false narratives with the intention of depressing Ukrainian morale and splitting support from abroad. The line between fact and fiction is becoming increasingly hazy as a result of the use of deepfake technology to produce plausible but fraudulent audio and video recordings, making countering Russian propaganda more difficult.

New Precedents in the Use of AI within Hybrid Warfare:

- Scalability and Automation: AI's ability to scale and automate hybrid warfare is one of the most important lessons to be learned from the Russia-Ukraine war. The ability of state and non-state actors to launch massive, automated assaults that concurrently target numerous sectors marks a significant advancement in their capabilities. This has created new guidelines for how future conflicts can play out, enabling more widespread and prolonged disruption through the use of AI-driven operations that can be started with little to no human involvement.
- Deniability and Ambiguity: The difficulty of attribution in hybrid warfare has been exacerbated by the employment of AI in cyber operations. Artificial intelligence has the ability to produce attacks that are hard to track down, giving attackers a plausible deniability. Russia's approach in Ukraine has been characterized by this ambiguity, which has made it more difficult for the international community to hold Russia responsible and take appropriate action[19].
- Influence on Global Security Dynamics: The dynamics of global security can be impacted by AI-enhanced hybrid warfare, as the Russia-Ukraine war has shown. In addition to having an immediate impact on the area, the battle has wider ramifications for NATO and other

[19] L. Dorosh, O. Ivasechko, J. Turchyn, *op. cit.*

international allies. Other countries have expanded their investment in AI and cyber capabilities as a result of the reevaluation of defense strategy brought about by the integration of AI into conflict. This has led to a change in the environment surrounding global security, as digital and AI-driven capabilities are increasingly complementing if not replacing traditional military might**.**

The current crisis in Ukraine provides important new information about how the world's security may develop, especially with the likelihood of AI being employed in hybrid warfare. It will become increasingly evident how AI technologies shape the course of wars as they develop, thus it is critical for governments to comprehend and get ready for the difficulties presented by AI-driven warfare. In a fast changing global security environment, the Russia-Ukraine war serves as a warning, emphasizing the need for comprehensive plans that handle the confluence of AI, cyberterrorism, and hybrid warfare[20].

Ethical and Legal Implications

Ethical Challenges

Significant ethical questions are raised by the employment of AI in hybrid warfare and cyberterrorism, especially in light of the potential effects on civilian populations and general human rights.1. These concerns are becoming more urgent as AI technologies develop and are used in more conflictual environments.

1. Civilian Impact and Collateral Damage: AI-driven cyberattacks have the potential to seriously hurt civilians, causing deaths and social unrest, by targeting vital infrastructure, such as electricity grids and hospitals. Attacks using AI are more precise, which raises questions about their validity and appropriateness[21].
2. Autonomy and Accountability: Making decisions and holding people accountable are difficult with autonomous AI systems. If an AI-driven strike results in unforeseen injury and maybe violates international humanitarian law, it becomes difficult to place culpability. This circumstance makes one worry about how human supervision and moral duty in combat are eroding.
3. Psychological and Social Impact: Deep fakes and AI-enhanced misinformation operations have the potential to sway public opinion, erode democratic processes, and create societal discord and

[20] W. Wróblewski, *op. cit*.
[21] J. Johnson, *op. cit*.

psychological anguish. Long-term peace and social stability are threatened by the dissemination of false information.

4. Escalation and Unintended Consequences: Artificial intelligence (AI) systems' quick decision-making can cause unintentional escalation of conflict before diplomatic measures can be taken[22]. Delegating important choices to machines raises ethical problems due to the possibility of AI-driven conflict spinning out of hand.

Legal and Regulatory Responses

International law is facing serious issues since existing legal and regulatory frameworks are unable to keep up with the incorporation of AI into cyberterrorism and hybrid warfare.

Current International Legal Frameworks**:**

- Cyber Operations: It is challenging to determine the origin of AI-driven assaults, which makes it more difficult to hold offenders accountable.
- Artificial Intelligence: The lack of global agreement on the moral application of AI in combat is impeding the creation of uniform legal guidelines.
- Hybrid Warfare: While there isn't a single treaty that specifically addresses hybrid warfare, it is governed by a number of current regulations that might not be sufficient to handle the problems brought on by AI integration.

Gaps and Challenges in Regulating AI:

- Attribution and Accountability: It is challenging to determine the origin of AI-driven assaults, which makes it more difficult to hold offenders accountable.
- Lack of Consensus on AI Ethics: The lack of global agreement on the moral application of AI in combat is impeding the creation of uniform legal guidelines.
- Regulating Autonomous Systems: The autonomy of AI systems is not taken into consideration by traditional legal frameworks, which makes it difficult to draft pertinent legislation.
- Ensuring Compliance: The clandestine nature of cyber operations and the difficulties in tracing AI usage make it difficult to enforce compliance with rules pertaining to AI.

In conclusion, there are difficult moral and legal issues raised by the use of AI in hybrid warfare and cyberterrorism. The international community has to work together to create new moral guidelines and legislative frameworks that

[22] L. Cladi, *Artificial intelligence and the future of warfare: the USA, China and strategic stability*, Defence Studies, 2021.

can keep up with technical developments while ensuring the safety of civilian populations and maintaining international security.

Countermeasures and Strategic Responses

Strengthening AI and Cybersecurity

Strong countermeasures must be developed as AI is increasingly incorporated into cyberterrorism and hybrid warfare in order to reduce dangers and improve international security. Protecting national and international interests from the increasing dangers posed by AI-enhanced cyber operations requires strengthening cybersecurity and AI-based defenses.

Improving AI-Based Defenses:

- AI-Driven Threat Detection: Using AI itself is one of the best strategies to combat cyberterrorism enhanced by AI. More swiftly and precisely identifying and neutralizing cyberattacks can be achieved with the development of sophisticated AI-driven threat detection systems. Large volumes of data can be analyzed in real time by these computers, which can identify trends, anomalies, and possible risks that human operators might overlook. Proactive protection against new assaults can be made possible by training machine learning algorithms to identify the telltale signs of certain cyber threats[23].
- AI in Intrusion Prevention and Response: Intrusion prevention systems (IPS) can potentially use AI to automatically react to threats that are discovered. These systems are capable of utilizing artificial intelligence (AI) to assess the type of attack and implement suitable defenses, like patching, isolating compromised computers, or obstructing hostile traffic. Artificial intelligence (AI) is more effective at thwarting future assaults and lessening the effects of successful breaches because of its capacity to adapt and learn from past events[24].
- Resilience and Redundancy: Adding resilience to vital infrastructure is yet another important tactic. AI can be used to create more robust systems that can resist cyberattacks and bounce back from them more quickly. This involves building fail-safes and redundant systems that can continue to perform vital tasks even in the event that main systems are damaged. Enhancing the overall security posture can be achieved by foreseeing possible sites of failure and developing systems that can withstand attacks.

[23] R. Das, R. Sandhane, *Artificial Intelligence in Cyber Security*, „Journal of Physics: Conference Series" 2021, Vol. 1964, Issue 4, 042072.
[24] I. Szabadföldi, *op. cit.*

The Role of AI in Detecting and Countering Hybrid Warfare**:**

- AI in Intelligence and Surveillance: AI may be very helpful in obtaining intelligence and conducting surveillance, which can aid in identifying and thwarting hybrid warfare tactics. AI is able to recognize signs of hybrid warfare activity, such as coordinated misinformation campaigns, military movements, or cyber incursions, by examining data from a variety of sources, including social media, satellite images, and communications intercepts. Making decisions more quickly and intelligently is made possible by this improved situational awareness.
- AI in Information Warfare: Artificial intelligence (AI) tools with the ability to recognize and destroy propaganda and deception are necessary to counter the information warfare element of hybrid warfare. Artificial intelligence (AI) algorithms can be used to track down the source of misleading or inaccurate information and monitor and evaluate internet material. Additionally, by boosting truthful information and diminishing the efficacy of opponents' misinformation campaigns, these tools can be utilized to launch counter-narratives.
- Automated Response Systems: AI can also be used to create automatic reaction systems that instantly respond to dangers posed by hybrid warfare. These systems offer a quick and scalable response to intricate hybrid threats by coordinating cyber defenses, deploying countermeasures, and managing information operations independently. These technologies can minimize the harm brought about by hybrid warfare operations by shortening the time between identifying a threat and putting a reaction in place by utilizing AI's speed and efficiency.

International Cooperation

Since hybrid warfare and AI-enhanced cyberterrorism are transnational threats, strong international collaboration is necessary to develop effective defenses. In order to ensure a coordinated response to emerging dangers and to build collective resilience, addressing these challenges through global collaboration is imperative.

Importance of International Collaboration:

- Shared Threat Landscape: Global challenges posed by cyberterrorism, artificial intelligence, and hybrid warfare cannot be resolved by individual nations acting alone. International collaboration is necessary for resource sharing, best practices, and intelligence sharing in order to implement effective countermeasures.
- Collective Security and Deterrence: International collaboration can improve deterrence against AI-driven hybrid warfare and fortify

collective security. By coordinating actions, governments can increase the costs and risks for potential aggressors, helping to avert escalations and defend international norms.

Proposals for New Cooperative Frameworks**:**

- Global AI and Cybersecurity Alliance: Form a formal partnership to promote cooperation on cybersecurity and AI-related challenges. In addition to promoting information exchange, cooperative research and development, and coordinated responses to cyber events, this alliance would seek to unify worldwide laws and regulations pertaining to AI technology.
- Information-Sharing Mechanisms: Establish safe, instantaneous lines of communication to share knowledge on upcoming attack techniques, countermeasures, and cyber threats. Improved communication of information would facilitate prompt reactions and lessen the effect of coordinated assaults.
- International Norms and Regulations for AI**:** Establish worldwide guidelines and standards that especially address artificial intelligence in military settings. Treaties or agreements that provide explicit criteria for AI research and application, such as prohibitions on autonomous weapons and best practices for responsible AI deployment, may be necessary to achieve this.
- Capacity Building in Developing Nations: Assist developing nations in strengthening their cybersecurity and AI capacities. Give these countries the tools, instruction, and technical support they need to bolster their defenses against complex hybrid threats and therefore contribute to international security.

In conclusion, a multimodal strategy that combines bolstering cybersecurity and AI defenses with promoting global collaboration is needed to tackle the issues raised by the confluence of AI, cyberterrorism, and hybrid warfare. The international community can better defend itself against the always-evolving threats posed by these technologies and guarantee a safer and stable world by building cutting-edge AI-driven defenses and new frameworks for international collaboration[25].

Conclusions

Summary of Key Findings

Several important conclusions that highlight the revolutionary influence of artificial intelligence (AI) on contemporary conflict have been drawn from this

[25] L. Cladi, *op. cit*.

investigation of the relationship between AI, cyberterrorism, and hybrid warfare.

1. AI's Role in Reshaping Cyberterrorism and Hybrid Warfare**:** Cyberterrorism is becoming more and more reliant on AI, which gives attackers more automation and scalability. In hybrid warfare, it combines with conventional tactics and informational methods to operate as a force multiplier[26]. The distinction between conventional and unconventional warfare is blurred by this convergence, posing significant difficulties for global security.
2. Global Security Implications: Significant obstacles are brought about by AI in hybrid warfare, including greater unpredictability, attribution issues, and risks of fast escalation. The war between Russia and Ukraine is a prime example of how AI-powered cyber operations may upend regional and international security. Reassessing and improving current security systems is necessary to counter these emerging threats.

Implications for Future Research and Policy

In order to make sure that the international community is ready to handle the new issues, there are crucial areas for future study and policy development as AI develops and becomes more prominently integrated into battle.

Suggestions for Further Research

- AI and Cyberterrorism Dynamics: Future studies should concentrate on the changing nature of AI-driven cyberterrorism, especially on the dual applications of AI in cyber operations. Research ought to examine how AI may anticipate and stop cyberattacks as well as the moral ramifications of applying AI to counterterrorism initiatives.
- AI in Hybrid Warfare Scenarios: Beyond the Russia-Ukraine conflict, a thorough examination of AI's participation in particular hybrid warfare situations is required. Studies that compare various conflicts and geographical areas may yield important insights on the application of AI in various geopolitical contexts and the implications for global security[27].
- Long-Term Consequences of AI in Warfare: The long-term effects of incorporating AI into combat, such as how it would affect international

[26] L. Herța, *op. cit*.
[27] D. Štrucl, *Russian Aggression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare*, „Contemporary MilitaryChallenges" 2022, Vol. 24, Issue 2, pp. 103-123.

law, human rights, and stability worldwide, should also be studied. Examining how AI might alter the essence of war itself, for as by reducing the threshold for conflict or spawning as-yet-undiscovered types of combat, is part of this[28].

Policy Recommendations

- Developing International AI Governance Frameworks: It is imperative that the international community moves swiftly to create all-encompassing governance frameworks for AI in military applications[29]. These ought to include moral standards, limitations on self-governing weapons, and procedures for openness and responsibility in AI-driven activities.
- Strengthening Cybersecurity Collaboration: Prioritizing international cybersecurity cooperation with an emphasis on coordinated defenses and strong information sharing is necessary[30]. Investments in cybersecurity technologies driven by AI are essential, and efforts should be made to guarantee that all countries, particularly developing ones, have access to the knowledge and resources they require.
- Ethical and Legal Oversight: It is necessary to set up independent organizations to supervise the moral and legal ramifications of AI in warfare. These organizations may guarantee adherence to global legal norms, offer directives for conscientious AI advancement, and foster dialogues on the implications of AI for policymakers, scientists, and civil society members[31].
- Investment in AI Research and Education: To better understand and mitigate the hazards associated with AI in hybrid warfare, governments and organizations should make investments in AI research and education.[32] This ought to encompass study on technology in addition to studies on international relations, ethics, and law.

In conclusion, artificial intelligence (AI) presents new hazards and ethical conundrums that need to be properly controlled, even as it offers considerable benefits in terms of improving capabilities in both cyberterrorism and hybrid warfare[33]. The international community may better handle the issues presented

[28] L. Dorosh, O. Ivasechko, J. Turchyn, *op. cit.*
[29] J. Johnson, *op. cit.*
[30] O. Ronzhes, *op. cit.*
[31] J. Johnson, *op. cit.*
[32] I. Szabadföldi, *op. cit.*
[33] K. Chung, *The Fourth Industrial Revolution and the US Initiative on the Future Warfare: Analyzing the Role of Artificial Intelligence and Autonomous Weapon System*, "Journal of International Politics" 2022, Vol. 13, Issue 2, 871.

by AI by encouraging more research and creating comprehensive policies, ensuring that the use of AI in battle is in line with humanitarian ideals and global security interests.

BIBLIOGRAPHY:

1. Beccaro A., *Modern Irregular Warfare: The ISIS Case Study*, "Small Wars & Insurgencies" 2018, Vol. 29, Issue 2
2. Chung K., *The Fourth Industrial Revolution and the US Initiative on the Future Warfare: Analyzing the Role of Artificial Intelligence and Autonomous Weapon System*, "Journal of International Politics" 2022, Vol. 13, Issue 2
3. Cladi L., *Artificial intelligence and the future of warfare: the USA, China and strategic stability*, Defence Studies, 2021
4. Das R., Sandhane R., *Artificial Intelligence in Cyber Security*, "Journal of Physics: Conference Series" 2021, Vol. 1964, Issue 4
5. Dorosh L., Ivasechko O., Turchyn, J., *Comparative Analysis of the Hybrid Tactics Application by the Russian Federation in Conflicts with Georgia and Ukraine*, "Central European Journal of International and Security Studies" 2019, Vol. 13, Issue 2
6. Hanratty K., *Artificial (military) intelligence: enabling decision dominance through machine learning*, "Defense + Commercial Sensing" 2023, Vol. 12538
7. Herța L., *Hybrid Warfare – A Form of Asymmetric Conflict, Sciendo: International conference KNOWLEDGE-BASED ORGANIZATION*, 2017, Vol. 23
8. Johnson J., *The AI Commander Problem: Ethical, Political, and Psychological Dilemmas of Human-Machine Interactions in AI-enabled Warfare*, "Journal of Military Ethics" 2022, Vol. 21, Issues 3-4
9. Pachankis Y., *Technical Analysis on the Cyber Organizational Criminology of Dictatorial Military Conducts – Experience from Human Trafficking and Coercions by Military Cyber Aggressions*, "International Journal of Security Privacy and Trust Management" 2022, Vol. 11, No. 3
10. Petrosyan M., *The Role of Non-State Actors in Modern Warfare: The Case of Syria and Nagorno-Karabakh*, "Journal of Balkan and Near Eastern Studies" 2023, Vol. 26, Issue 2
11. Ronzhes O., *The role of digital technologies in the adaptation of citizens of Ukraine to military aggression by the Russian Federation*, "Scientific Studios on Social and Political Psychology" 2022, Vol. 28, No. 2

12. Sharma P., Sarma, K., Mastorakis N., *Artificial Intelligence Aided Electronic Warfare Systems- Recent Trends and Evolving Applications*, "IEEE Access" 2020, Vol. 8
13. Štrucl D., *Russian Aggression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare*, "Contemporary Military Challenges" 2022, Vol. 24, Issue 2
14. Szabadföldi I., *Artificial Intelligence in Military Application – Opportunities and Challenges*, "Land Forces Academy Review" 2021, Vol. 26, Issue 2
15. Workman H., Dalaklis D., Ávila-Zúñiga-Nordfjeld A., *Russia/Ukraine military conflict: Discussing the maritime element of the confrontation*, "American Yearbook of International Law" 2023
16. Wróblewski W., *Terrorism and the Hybrid Warfare in Aspect of War in Ukraine*, "Polish Political Science Yearbook" 2022, 2022, Vol. 51, Issue 4
17. Zhang Y., Dai Z., Zhang L., Wang Z., Chen L., Zhou Y., *Application of Artificial Intelligence in Military: From Projects View*, 6th International Conference on Big Data and Information Analytics (BigDIA) 2020

„Ante Portas – Security Studies”
2024, No. 21
DOI: **10.33674/1202417**

Svitlana KONSTANTYNYUK[1]
Ukraine

BETWEEN SOFT AND HARD POWER: THE ESSENCE OF PUBLIC DIPLOMACY AS A SECURITY TOOL

Abstract: *The article presents a theoretical and conceptual analysis of public diplomacy as a tool for safeguarding state security interests. Employing an actor-centred approach, the paper proposes the operationalization of public diplomacy functions within the security dimension and analyses the applicant-actor's strategies in utilizing public diplomacy to address modern security challenges and protect its interests. The article structurally outlines the advantages and risks associated with various forms and practices of public diplomacy. It argues that in the context of the transformation of the global order and the intensification of hybrid warfare, public diplomacy should be regarded as a fully-fledged security tool used by actors to defend against external destructive influences and to engage in counteraction. This perspective provides grounds to view media diplomacy as an instrument of soft power and hard power.*

Keywords: *Public diplomacy, security, challenge, soft power, hybrid warfare, media, propaganda, culture diplomacy, information warfare, cognitive warfare, hard power.*

Introduction

In the era of information and psychological, cognitive, discursive, and narrative wars, and at the same time, the transformation of the world order, studies of non- “hard” methods of state influence on other actors in the international arena are becoming increasingly relevant. Public diplomacy (hereinafter: PD) as one of the soft power instruments plays a crucial role in

[1] Svitlana Konstantynyuk, MA, Yuriy Fedkovych Chernivtsi National University (Ukraine), ORCID: 0009-0007-1889-8401, email: konstantyniuk.svitlana@chnu.edu.ua

influencing allies and opposition and also acts as an important preventive tool in overcoming potential challenges and threats at the foreign and domestic level. For example, an interesting observation of Illya Havrylenko is that active US public diplomacy in certain regions was correlated primarily with the identification of certain threats to US national security[2].

The tendency to use PD as a manifestation of soft power, or within the framework of smart power, when it plays a reinforcing function, is, on the one hand, a necessity for great powers to defend their legitimacy. For example, in the context of the current Cold War 2.0, this process is most noticeable, as it is accompanied by the build-up of China's soft power on the one hand, and the US intentions to contain its opposition on the other. These processes, which, of course, involve other actors, lead to the understanding of PD and soft power within the framework of "hard" influence, because, first, they are used as a means of confrontation, and second, as a means of protection.

This view leads to the idea that although PD and propaganda are incompatible both from an ontological and practical point of view, PD is manipulative because of its ability to influence the perception of certain political processes by wide audiences. However, unlike propaganda, PD is more invisible and has a more long-term effect. In one of her speeches in 2009, Deputy Secretary of State Judith McHale aptly noted: "This is not a propaganda contest – it is relationship race"[3]. Public diplomacy in all its diversity is aimed at interacting with the audience, understanding its needs and moods, and depends on its reaction. This interaction is the basis for building trusting relationships, which is the goal of PD, and increasing the attractiveness of the actor who channels soft power.

The same need arises for peripheral and semi-peripheral states that do not have enough resources and capabilities to fully broadcast their favourable narratives and messages to the world. Such actors are more vulnerable to foreign information and mass cultural influences, especially if they come from stronger states. Accordingly, PD becomes a necessary tool for protecting the domestic audience on the one hand, and on the other hand, it ensures the protection of their interests abroad. The most relevant example today is Ukraine, which, despite its low soft power potential, was able to secure the commitment of allies and partners at the beginning of the full-scale Russian invasion, including through public diplomacy practices that were applied at all levels of foreign audiences – from the political elites of Western partner countries and their societies, which have a direct impact on decision-making

[2] I. I. Havrylenko, *Heopolitychnyi vymir publichnoi dyplomatii SShA*, "Mizhnarodni vidnosyny" Seriia "Politychni Nauky" 2014, No. 3, pp. 25-38.

[3] N. Snow, *Public Diplomacy in a National Security Context*, "The Routledge Handbook of Security Studies" 2017, 2nd edition, p. 410.

within the democratic system.

These observations, which indicate the contextual nature of the use of PD, necessitate a more detailed analysis of it as a security tool of the state. The deepening of the theoretical and conceptual understanding of PD leads not only to the improvement of the methodological tools of the study but is also important for practitioners, especially in the field of protecting the security of the state, society and the individual.

Public Diplomacy as a National Security Tool

PD should be understood as a tool used by an actor (state, organization and non-state actors) "[…] to understand cultures, attitudes, and behaviours, build and manage relationships, and influence opinions"[4]. As a foreign policy practice, PD has a wide range of manifestations and actors involved, which makes it a difficult object for quantitative analysis, but given the tendency to use soft methods of influence on other actors, it requires considerable attention from both practitioners and scholars. Today, as noted by Nancy Snow, the PD is as essential as the military readiness of the state[5].

The subjects of public diplomacy are as diverse as its forms and methods of implementation. For example, in 2016, the US Advisory Commission on Public Diplomacy noted that the involvement of young people, civil society representatives, opinion leaders, and journalists is a critical factor in effective public diplomacy, especially in the context of global ideological conflict, which, in turn, challenges not only the national security of individual actors but also the liberal order as a whole[6]. The security context of the PD is growing, and even more so in the context of the unstable international world order.

If we talk about the normative aspects of the use of PD, we should pay attention to the heterogeneity of motives and intentions for its use. For example, Alan K. Henrikson identifies the following strategies of public diplomacy: 1. consolidation (interaction with partner countries); 2. deterrence (both tactical and strategic); 3. penetration (to the audiences needed by the applicant actor); 4. expansion (dissemination of cultural goods, values, messages, and ideas); 5. transformation (direct influence that leads to

[4] R. Desai-Trilokekar, E. H. Masry, *The Nexus of Public Diplomacy, Soft Power, and National Security: A Comparative Study of International Education in the U.S. and Canada*, "Journal of Comparative & International Higher Education" 2022, Vol.14, Issue 5, p. 113.

[5] N. Snow, *U.S. Public Diplomacy: Its History, Problems, and Promise*, "Readings in Propaganda and Persuasion: New and Classic Essays", Pub. Sage 2006, p. 7.

[6] S. MacDonald, *Soft Power Today Measuring the Influences and Effects*, The Institute for International Cultural Relations, October 2017, pp. 14-15.

qualitative changes in the behaviour of the recipient actor)[7]. Such a taxonomy of strategies is necessary to understand both the motives of the applicant actor in using soft power and to determine the necessary behaviour in solving the state's security problems. However, at the same time, it is a reason to consider PD not only as a reputational, image and branding tool but also as a full-fledged means of conducting information, cognitive and discursive wars of our time.

Accordingly, considering Artem Patalach's aggregate analytical model, which considers the interaction of the applicant and recipient actor, as well as the behaviour of the competing actor[8], the following functions of PD towards different audiences can be formulated (tab. 1):

Tab. 1. Operationalization of public diplomacy functions within the framework of ensuring national security

Regarding allied and partner actors	***Regarding competing actors***	***Regarding internal audience***
Consolidation function	Proactive function	The function of including non-state actors in the state's foreign policy activities
The function of deepening socio-cultural, economic, scientific (etc.) dependence	The function of establishing favourable relations	The function of mobilization of diplomatic missions and non-state actors abroad in influencing the formation of the state's perception
Explanatory function	The function of information and psychological influence on the enemy's population	The function of informing about foreign policy interests
The function of forming security agendas	Self-desecuritization function	The function of developing assertive abilities of the population in responding to external destructive influences

[7] K. A. Henrikson, *What Can Public Diplomacy Achieve?* "Discussion Papers in Diplomacy" 2006, No.104, Netherlands Institute of International Relations, p. 7, <https://www.jura.fu-berlin.de/fachbereich/einrichtungen/oeffentliches-recht/lehrende/bolewskiw/dokumente/1_Creative-Diplomacy/Henrikson_what_can_public_diplomacy_achieve.pdf> (30.11.2024).

[8] A. Patalakh, *Assessment of Soft Power Strategies: Towards an Aggregative Analytical Model for Country-Focused Case Study Research*, "CIRR" 2016, Vol. 76, p. 87.

Securitization function	Deterrent function	The function of reflecting oneself in the positive experience of being seen by other actors

Source: Own source

If we take into account the above-proposed functions of the PD in the context of interaction with partners and allies, its main task is partnership sustainability. While consolidation and deepening of interdependence is the basis of the common good of any sustainable and long-term partnership and can bring dividends to all its participants, the function of securitization, shaping the security discourse favourable to the applicant actor, and explaining the applicant actor's own foreign policy decisions can be manipulative. For example, during the active struggle against terrorism in the United States and the destabilization of the Middle East in the new century, their PD performed these functions, which was to legitimize US foreign policy decisions among its closest partners in the EU. However, attempts to unite the West against the threat of terrorism cannot be called successful, which points to the need to find more thoughtful and sophisticated approaches to shaping the strategy of the PD in cases of both collective and self-security.

Considering the functions of the PD concerning competing actors, it is worth emphasizing its offensive nature. The anticipatory function, for example, allows the applicant actor to gain primacy in interpreting and broadcasting its own, favourable vision of events and phenomena, as well as in assessing its own foreign and domestic policy decisions in the global media space. The content and context of the PD will depend on the recipient actor, but it may contain practices that harm the reputational security of the competing actor among its allies and neutral actors. Instead, the functions of self-desecuritization and deterrence are more likely to be a reaction of the applicant actor to the use of negative soft power by a competing actor and help to establish trusting relations with those actors that are in the zone of political interests of both competing or conflicting parties. At the same time, the ability to use stable information and mass-cultural influences on the competitor's population is important, especially for states claiming world leadership. Just as during the Cold War, especially in its final phase, US mass culture played the role of a Trojan horse in the competition for the sympathies of the Soviet population, so in Cold War 2.0 we can see attempts by competing parties to influence each other's audiences through the dissemination of cultural and informational goods. The practice of PD, whose normatively positive perception is often useful for certain actors to mask their intentions, becomes their guide.

The effects of the external orientation of the PD on the internal audience of the applicant actor are poorly researched. However, it is worth recognizing that

a positive experience of a state's PD abroad can have a positive domestic political effect. For example, civil society, opinion leaders, artists, and celebrities become actors of the PD and thus take on the task of informing, explaining, and promoting the interests of the state, including security interests, not only abroad but also at home. This, in turn, contributes to a better awareness of the domestic audience of the state's security priorities. This practice, accordingly, helps to maintain the population's resilience to hostile information and psychological influences and can contribute to greater trust in the government. In addition, a positive perception of the state by other actors gained through effective PD, is an important component of self-perception, as it contributes to a positive experience of identifying with one's country. For example, the heroic vision of partner countries and the support of allies for Ukraine at the beginning and throughout the Russian full-scale invasion had a direct impact on the resilience and consolidation of the Ukrainian people at a critical time.

Having formulated the main functions of the PD in the security dimension, it is worth paying attention to possible models of using the PD in the security interests of the state. The division into the following types of interrelationship between the SP and public diplomacy as its main instrument with national security, proposed by Roopa Desai-Trilokekar and Hani El Masry:

1. Conflicting: harsh and sharp instruments offset the efforts of public diplomacy, making it useless or ineffective;
2. Complementary: SP acts as a factor of reputational security;
3. Securitized: public diplomacy becomes a tool of defense;
4. Conditioned by "smart power": a balanced combination of soft power and hard forms of influence;
5. National security conditioned by the involvement/integration of soft power: attention of the claimant actor to both the projection of its soft power and the soft power of other actors that articulates in the space of the actor-claimant[9].

Thus, based on the above operationalization, it can be concluded that PD becomes effective for security protection only when it is consciously used (directly or indirectly) as a security instrument. In case of failure to ensure a reasonable PD strategy, which is based on the foreign policy agenda of the applicant actor and takes into account the peculiarities of relations with a particular recipient actor, attempts to influence its perception may be futile or even undermine the latter's trust.

A well-known researcher of soft power and public diplomacy, as well as the author of the concept of "reputational security" Nicholas J. Cull, analyzing the practices of PD in the era of the COVID-19 pandemic, identifies four strategies

[9] R. Desai-Trilokekar, E. H. Masry, *op. cit.*, pp. 114-115.

of public diplomacy of claimant actors:

1. self-praise (emphasis on successful experience in combating threats);
2. criticizing others (emphasizing the failures of other actors to promote one's (more) positive experience in dealing with threats);
3. engaging others through gifts/public diplomacy of actions (manifested in the provision of humanitarian, and financial assistance to the recipient actor, which signals increased cooperation);
4. multilateral cooperation (consolidation and unification of partners to address common challenges and problems)[10].

It can be assumed that the theoretical differentiation of the "soft" behavior of the claimant actor to protect its security interests, presented above, is also relevant for the analysis of other security contexts. For example, the US public diplomacy of action, namely humanitarian aid, has worked effectively in predominantly Muslim Indonesia. Two years after the 2004 tsunami, a survey of Indonesian perceptions of the United States showed a threefold increase in sympathy for the United States and a significant decline in support for Osama bin Laden[11]. Another example of the success of the public diplomacy of action strategy is the U.S. military assistance to Japan after the earthquake, tsunami and nuclear power plant accident, which included humanitarian support and assistance in restoring infrastructure. A 2011 poll of Japanese citizens showed a significant increase in favorability toward the United States (85%), which remains stable[12].

Security aspects of public diplomacy practices and forms

So, given the regularity of the importance of using public diplomacy in protecting the security interests of the state, the following table of potential benefits and risks of various manifestations of PD is offered for review (tab. 2):

Tab. 2. Benefits, opportunities and risks of public diplomacy practices and manifestations

	Potential benefits and opportunities	**Risks**
	1. Acts invisibly	1. Hostile perception of the

[10] N. J. Cull, *From Soft Power to Reputational Security: Rethinking Public Diplomacy and Cultural Diplomacy for a Dangerous Age*, "Place Branding and Public Diplomacy*"* 2022, Vol. 2018, pp.18-21.

[11] M. Wallin, *The New Public Diplomacy Imperative. America's Vital Need to Communicate Strategically,* New York "American Security Project" 2012, p. 16.

[12] N. Snow, *Public Diplomacy in…*, *op. cit.*, p. 410.

Cultural diplomacy	2. Promotes a simplified perception of the norms, values, and socio-cultural characteristics of the state	cultural product (for example, the perception of the distribution of certain cultural goods as cultural imperialism by the recipient actor) 2. Inability to decode certain cultural goods in the cognitive space of the recipient actor
Sport diplomacy	1. Accessibility to wide audiences 2. Demonstration of mutual respect	1. Prohibition of participation in international sports competitions 2. Image and reputational losses
Education and science diplomacy	1. Ability to influence young people through educational exchanges 2. Creating a sense of belonging among allied actors 3. Demonstration of the actor's ability to solve security problems and formulate a security agenda 4. Significant image dividends 5. Reducing the radicalization of young people	1. The use of scientific achievements by other countries and theft of innovations 2. The need to limit exchange opportunities for representatives of hostile countries, which increases the conflict potential of relations
Military and defense diplomacy	1. Ensuring regional influence 2. Promoting consolidation of partners 3. Participation in training of partners to manage their security 4. Indirect participation in military operations (through consulting, military exercises) 5. Preventing crises and minimizing hostility	1. Perception by a competing actor of increased military diplomacy with partners as an immediate threat 2. Theft of the latest developments in military technology 3. Incompatibility of goals, objectives, and motives of interacting actors
	1. Formation of favourable narratives and an attractive	1. Rejection of content by the audience (apathy, criticism,

Media diplomacy, cyber diplomacy and twiplomacy	image of the state as a tool for protection against hostile influences 2. Rapid response to security challenges 3. Proximity to the audience 4. Creation of a security agenda and fixation on security problems 5. Flexibility in formulating and adjusting the problematic discourse	resistance) 2. Information operations to destabilize the information space
Domestic public diplomacy	1. Ensures internal consolidation and assertiveness to foreign information and mass-cultural interventions 2. Mobilization of the internal audience in the creation of the "SP", including civil society	1. Poorly thought-out communication strategy, the unwillingness of opinion leaders to interact 2. Misunderstanding/rejection of the existing security discourse by the population and lack of interest in mechanisms for solving security problems and challenges 3. Lack of competencies in the field of media literacy in society 4. Prevailing information, psychological and cultural activities of the competing actor in terms of effectiveness 5. "Black swan" effects

Source: Own source

Having analyzed the essence of public diplomacy as a national security tool, as well as having identified the main potential benefits and risks of using certain types of PD practices, it is necessary to consider their specific features in more detail.

Cultural diplomacy occupies a prominent place in both scholarly discourse and practice, as the dissemination and popularization of cultural goods involves

the widest possible audiences and can influence the recipient actor most imperceptibly. The ability to influence world views, political assessments and preferences, and even lifestyles has been the subject of many scholarly works, but even such a soft tool as cultural diplomacy requires its practitioner to understand the context of its use. Flexibility and the ability to manifest itself in the non-political sphere for the recipient are important for effective soft power. For example, Russia's PD before the full-scale invasion of Ukraine, which was certainly regionally differentiated, did not provide the results Russia expected. Victoria Hudson's 2015 study demonstrated an identical skeptical discourse among young people in eastern Ukraine that is characteristic of the Western regions[13]. As Olena Komar aptly notes, Russian soft power is "[…] a continuation of propaganda by attractive means"[14]. However, soft power, as noted earlier, although manipulative, has little to do with propaganda. That is why there is a view of cultural diplomacy as a set of practices that allows dominant countries to consolidate their norms and values abroad on an imperialist basis[15]. Accordingly, the main task of the applicant actor (especially those with a high soft power potential) is to neutralize this side effect in the recipient's perception.

The scientific sphere has also become a more tangible security tool, because in the context of the current confrontation between superpowers, the development of new technologies and leading research is "[…] an element of defence, or the achievement of the goal of becoming a world power"[16]. German scholars also emphasize that scientific and educational diplomacy play a key role in creating a sense of belonging to the liberal order among allies[17]. This is confirmed by the thesis that the United States has always approached international educational exchange as a factor that promotes mutual support and security interests[18]. An example is the Fulbright program during the Cold War.

In addition, educational and scientific exchanges are a potential factor in

---

[13] V. Hudson, *"Forced to Friendship"? Russian (Mis-)Understandings of Soft Power and the Implications for Audience Attraction in Ukraine*, "POLITICS*"* 2015, Vol. 35, Issue 3-4, p. 10.

[14] O. Komar, *Soft Power i propahanda u Rosiisko- Ukrainskii viini: epistemolohichnyi analiz*, "Ukrainoznavchyi almanakh" 2022, Vyp. 30, p. 86.

[15] T. Mirrlees, *American Soft Power, or, American Cultural Imperialism?*, ed. C. Mooers, *The new imerialists: Ideologies of empire*, Oneworld Publications, Oxford 2006, p. 199.

[16] J. Mukherjee, *Die Wissenschaft muss sich ihrer Bedeutung für die nationale Sicherheit bewusst sein*, "49 Security: Impulse für die Nationale Sicherheitsstrategie", <https://fourninesecurity.de/2022/09/26/die-wissenschaft-muss-sich-ihrer-bedeutung-fuer-die-nationale-sicherheit-bewusst-sein> (30.11.2024).

[17] H. K. Anheier, E. L. Knudsen, R. A. List, *Soft Power und die neue Geopolitik: Germany in vergleichender Perspektive*, „ifa ECP Monitor", Stuttgart 2023, p. 5.

[18] R. Desai-Trilokekar, E. H. Masry, *op. cit.*, p. 119.

reducing extremist views and improving the image[19]. For example, one of the Atlantic Council's 2018 reports recommends that the US government immediately establish educational and scientific exchanges with young people in Sudan who, in isolation, are committed to anti-Americanism, and thus prevent destructive consequences in further interstate cooperation[20].

The notion of domestic public diplomacy emerged not so long ago, but the growing information and mass-cultural influence on the domestic audience of the applicant actor necessitates the development of tools to develop assertive abilities among the population and mobilize the audience in the creation of soft power. In addition, the low level of well-being and dissatisfaction with various aspects of the country's population can become an "Achilles' heel" in the state's attempts to magnetize attention. At the same time, according to German researchers, today people are increasingly affected by global actions or inaction, which necessitates the government to explain and discuss its foreign policy decisions to the public[21]. Another important aspect pointed out by Margaret Seymour is that the solution to the US domestic problems can reflect the goals of its foreign policy, which will result in protecting the American people from threatening operations and strengthening confidence abroad[22]. However, it can be assumed that domestic public diplomacy is more intensively used to consolidate society in non-democratic systems. For example, the "Chinese dream" is also primarily a tool for consolidating society in China, and only then a projection of itself to the world. No wonder Hu Jintao, in one of his speeches, defines the cultural development of soft power as a means of fighting for national power[23]. Indeed, it is quite clear that China's soft power is an essential component of regime stability and is used as a convincing argument in its favour in the context of avoiding public discontent. Nicholas J. Cull rightly points out: "Intense political divisions are another matter and constitute a much greater danger to the reputational security of the country than stories invented by enemies"[24].

In addition to the above-mentioned aspects, public awareness of the state's

---

[19] *Ibidem*, p. 128.

[20] T. Carney, M. C. Yates, *Sudan: Soft Power, cultural engagement, and national security*, "Atlantic Council" March 8, 2018, p. 10.

[21] N. Renvert, M. Herkendell, J. Dahm, u.a., *Frieden, Sicherheit und Soziale Demokratie,* Bonn: Friedrich-Ebert-Stiftung, Dezember 2017, p. 76.

[22] M. Seymour, *Building Soft Power Back Better?* "Foreign Policy Research Institute", <https://www.fpri.org/article/2021/03/building-soft-power-back-better/> (30.11.2018)

[23] W. Zhang, *China's cultural future: from soft power to comprehensive national power*, "International Journal of Cultural Policy" 2010, Vol. 16, No. 4, p. 398.

[24] N. J. Cull, *Public Diplomacy and the Road to Reputational Security: Analogue Lessons from US History for a Digital Age*, Williamsburg, VA "AidData at William & Mary" 2022, p. 21.

security priorities is also important, as it determines the security orientation of society. Thus, strengthening institutions and civil society and ensuring economic development play an essential role for security, especially for fragile states[25]. Nancy Snow, in a work that focuses on public diplomacy as a security tool, points out that the threat of terrorism is a lesson that an informed and globally active, as well as a consolidated American public is a key component of US security[26]. This, in turn, is evidence that effective soft power should also be seen as a domestic political tool. The Concept of the State Targeted Program for the Formation of a Positive International Image of Ukraine for 2013-2015 states, in particular, that a positive vision of the state by the world community contributes to raising the level of self-awareness, strengthening social unity, and socio-economic transformations[27], which, as it turned out for Ukraine on February 24, 2022, is a great resource in its ability to withstand large-scale threats. Ironically, Joseph Nye in his latest work refers to the following thesis: "Security is like oxygen: you do not tend to notice it until you begin to lose it"[28]. Another example of realizing the importance of positive foreign perceptions for domestic attitudes is the understanding of NATO's PD. For example, Article 2 of The North Atlantic Treaty refers not only to the development of peaceful and friendly international relations but also to the promotion of conditions for internal stability and prosperity[29].

However, other actors' perceptions of the applicant may have more tangible effects than domestic actors' understanding of the attractiveness of the state and alliances and their subsequent identification with the subject of this attractiveness, namely, to influence domestic and foreign policy decisions. N. Cull, the author of the concept of "reputational security," provides an example of such an effect, which is the reverse of the applicant actor's reaction to other actors' perception of themselves: the key to solving racial problems and expanding civil rights for Dwight Eisenhower and John Kennedy administrations was concern about the construction of the state's international image[30]. Accordingly, the degree of reaction of the recipients of PD and soft power can influence domestic and foreign policy decisions of states, primarily in the name of image and reputational dividends.

---

[25] A. N. Uste, U. S. Aydin, *New Dimensions of Soft Power in the 21st Century*, "Interdisciplinary Journal of Research and Development" May 2023, Vol. 10, No. 1, p. 201.
[26] N. Snow, *U.S. Public Diplomacy: Its History …*, *op. cit.*, p. 237.
[27] D. S. Korotkov, *Kontseptsiia «m'iakoi syly» v konteksti zovnishnopolitychnoi stratehii Ukrainy*, Naukovo-teoretychnyi almanakh "Hrani" 2018, Vol. 21, Issue 9, p. 135.
[28] J. S. Nye Jr., *Soft Power and Great-Power Competition. Shifting Sands in the Balance of Power Between the United States and China*, Springer 2023, p. 132.
[29] The North Atlantic Treaty, *NATO*, April, 4, 1949, <https://www.nato.int/cps/en/natohq/official_texts_17120.htm> (30.11.2018).
[30] N. J. Cull, *Public Diplomacy …, op. cit.*, p. 3.

Cyber diplomacy, as well as media diplomacy, play a crucial role in shaping favourable narratives and an attractive image of the state as a tool for protection against hostile influences, especially in the digital age[31]. In addition, cyber diplomacy makes it possible to create joint multilevel infospheres between allies, which ensures even greater interdependence. For example, the US Tor project, developed by the US Naval Research Laboratory, provides foreign users with software for anonymity in communication and data transmission, thus bypassing state censorship[32]. This practice should be attributed to the US soft power, as it provides concrete opportunities to realize benefits such as the freedom to seek, reproduce, and share information, which contrasts with the lack of such opportunities in authoritarian states. Media diplomacy is distinguished by the ability to broadcast the necessary messages and narratives to a wide audience, which requires a preliminary study of the specifics of the recipient. For example, in 2002, to improve the image of the United States, several videos were published (as part of the Common Values Initiative) to demonstrate respect for Islam by describing the positive experience of Muslims in the United States[33]. This material was broadcast in the Middle East and Asia but was doomed to failure because it did not meet the needs of the target audience[34].

Defence and military diplomacy is also a significant component of a state's soft power. Here we should refer to the work of Kyle J. Wolfley, who argues that a state's military potential is a factor in attracting and persuading other actors and is important for understanding modern international competition[35]. The main ways of "soft power" that the researcher identifies are: 1. engaging allies; 2. influencing the values and roles of other states' militaries through socialization; 3. training other armies and delegating security tasks to other actors; 4. managing allies' behaviour through security guarantees[36]. Lech Drab defines defensive diplomacy as a significant mechanism for crisis prevention, international prevention and international security, as well as a tool for

[31] U. Bergmane, *Public Diplomacy as a National Security Tool*, "Foreign Policy Research Institute" 2017, <https://www.fpri.org/article/2017/05/public-diplomacy-national-security-tool/> (30.11.2018)
[32] M. Wallin, *op.cit.*, p. 20.
[33] *Ibidem*, p. 12.
[34] *Ibidem*.
[35] J. K. Wolfley, *The Shape of Things to Come: Why the Pentagon Must Embrace Soft Power to Compete with China*, "Modern War Institute" 2021, <https://mwi.westpoint.edu/the-shape-of-things-to-come-why-the-pentagon-must-embrace-soft-power-to-compete-with-china/> (30.11.2018).
[36] *Ibidem*.

minimizing hostility[37]. However, given their non-normative nature, soft power and public diplomacy within the defence and military sphere should not be viewed as exclusively peacekeeping practices. For example, the US Office of Strategic Influence uses soft power as a strategic and tactical tool in confronting rival countries[38].

Thus, having analysed different types of manifestations of PD, we can conclude that PD, in comparison with other types of non- "hard" influence, can take over the task of protecting national interests at all levels, having an impact on the perception of not only the political establishment of the recipient actor but also on the formation of the opinion of the applicant actor by the population. The multifaceted nature of its manifestations, as well as the number and diversity of PD agents and, accordingly, its recipients, demonstrate the high potential of this tool in protecting the state's security in both the short and long term. Thus, it can be argued that PD, in contrast to more aggressive forms of influence (such as propaganda, black PR, disinformation, etc.), is a safer means of winning minds and hearts around the world.

Conclusion

Given the above considerations, we can conclude that in the time of transformation of the world order, characterized by tensions between superpowers, PD occupies a prominent place not only in foreign policy but also in the domestic security dimension. Although the multifaceted nature and diversity of the forms and manifestations of PD require the scientific community to develop a more accurate methodological map of its study, it is necessary to understand the behavior and motives of the actors that direct it. There is also a need to theoretically and practically improve its mechanisms and understand the criteria for its effectiveness in specific historical cases.

It should also be noted that although PD is the main instrument of soft power, it should be seen as a means of achieving the actor's goals in the security dimension without burdening PD with normative moral and ethical functions. In an era when the concept of propaganda is giving way to more subtle cognitive influences, and phenomena such as fake news and disinformation within the framework of information and cognitive wars do not play a decisive role in the long run, it is the practice of public diplomacy that operates discreetly that becomes both a tool for displacing the influence of rival actors and a means of strengthening relations with allies. In addition, within the framework of the actor's PD, the practice of public diplomacy, which in theory

[37] L. Drab, *Defence diplomacy – an important tool for the implementation of foreign policy and security of the state*, "Security and Defence Quarterly" 2018, Vol. 20. No. 3, pp. 59-61.
[38] T. Mirrlees, *op. cit.*, p. 212.

is aimed at an external recipient, brings significant dividends for the internal audience - both in the context of involving civil society and the population in participating in the practice of PD and in the context of positive experience in perceiving oneself at the normative, cognitive and affective levels.

At the same time, it should be noted that although PD is aimed at improving the recipient actor's perception of the applicant actor, the public diplomacy strategy should be balanced and formulated, as well as based on the context of relations with a particular recipient actor and its interests. Otherwise, if such data are not taken into account, both for large states and states with low soft power potential, the use of this tool to influence the perception of other actors may not bring the desired results or even have negative consequences in further forming relations.

BIBLIOGRAPHY:

1. Anheier H. K., Knudsen E. L., List A. R., *Soft Power und die neue Geopolitik: Germany in vergleichender Perspektive*, ed. H. K. Anheier und ifa, "Der External Cutural Policy Monitor", Stuttgart 2023
2. Bergmane U., *Public Diplomacy as a National Security Tool*, "Foreign Policy Research Institute" 2017, <https://www.fpri.org/article/2017/05/public-diplomacy-national-security-tool/>
3. Carney T., Yates M. C., *Sudan: Soft Power, cultural engagement, and national security*, "Atlantic Council" March 8, 2018
4. Cull N. J., *From Soft Power to Reputational Security: Rethinking Public Diplomacy and Cultural Diplomacy for a Dangerous Age*, "Place Branding and Public Diplomacy", 2022, Vol. 18
5. Cull N. J., *Public Diplomacy and the Road to Reputational Security: Analogue Lessons from US History for a Digital Age*, "AidData at William & Mary", Stuttgart 2022
6. Desai-Trilokekar R., Masry E. H., *The Nexus of Public Diplomacy, Soft Power, and National Security: A Comparative Study of International Education in the U.S. and Canada*, "Journal of Comparative & International Higher Education" 2022, Vol.14, Issue 5
7. Drab L., *Defence diplomacy – an important tool for the implementation of foreign policy and security of the state*, "Security and Defence Quarterly*"* 2018, 20(3)
8. Havrylenko I. I. *Heopolitychnyi vymir publichnoi dyplomatii SShA*, "Mizhnarodni vidnosyny", Seriia "Politychni Nauky" 2014, No. 3, <http://journals.iir.edu.ua/index.php/pol_n/article/view/2240>
9. Henrikson K. A., *What Can Public Diplomacy Achieve?* "Discussion Papers in Diplomacy" 2006, No. 104, Netherlands Institute of International

Relations, <https://www.jura.fu-berlin.de/fachbereich/einrichtungen/oeffentliches-recht/lehrende/bolewskiw/dokumente/1__Creative-Diplomacy/Henrikson_what_can_public_diplomacy_achieve.pdf>
10. Hudson V., *"Forced to Friendship?" Russian (Mis-)Understandings of Soft Power and the Implications for Audience Attraction in Ukraine*, "POLITICS" 2015, Vol. 35, Issue 3-4
11. Komar O., *Soft Power i propahanda u Rosiisko- Ukrainskii viini: epistemolohichnyi analiz*б "Ukrainoznavchyi almanakh" 2022, Vyp. 30
12. Korotkov D. S., *Kontseptsiia «m'iakoi syly» v konteksti zovnishno-politychnoi stratehii Ukrainy*, Naukovo-teoretychnyi almanakh "Hrani" 2018, Vol. 21, Issue 9
13. MacDonald S., *Soft Power Today Measuring the Influences and Effects,* The Institute for International Cultural Relations, October 2017
14. Mirrlees T., *American Soft Power, or, American Cultural Imperialism?*, ed. C. Mooers, *The new imperialists: Ideologies of empire*, Oneworld Publications, Oxford 2006
15. Mukherjee J., *Die Wissenschaft muss sich ihrer Bedeutung für die nationale Sicherheit bewusst sein*, „49 Security: Impulse für die Nationale Sicherheitsstrategie" 2022, <https://fourninesecurity.de/2022/09/26/die-wissenschaft-muss-sich-ihrer-bedeutung-fuer-die-nationale-sicherheit-bewusst-sein>
16. Nye S. J., *Soft Power and Great-Power Competition. Shifting Sands in the Balance of Power Between the United States and China*, Springer 2023
17. Patalakh A., *Assessment of Soft Power Strategies: Towards an Aggregative Analytical Model for Country-Focused Case Study Research*, "CIRR" 2016, Vol. 76
18. Renvert N., Herkendell M., Dahm J. u.a., *Frieden, Sicherheit und Soziale Demokratie*, Bonn: Friedrich-Ebert-Stiftung, Dezember 2017
19. Seymour M., *Building Soft Power Back Better?*, "Foreign Policy Research Institute" 2021, <https://www.fpri.org/article/2021/03/building-soft-power-back-better/>
20. Snow N., *U.S. Public Diplomacy: Its History, Problems, and Promise*, "Readings in Propaganda and Persuasion: New and Classic Essays", Pub. Sage 2006
21. Snow N., *U.S. Public Diplomacy in a National Security Context*, "The Routledge Handbook of Security Studies" 2017, 2nd edition
22. The North Atlantic Treaty, NATO, April 4, 1949 <https://www.nato.int/cps/en/natohq/official_texts_17120.htm>
23. Uste A. N., Aydin U. S., *New Dimensions of Soft Power in the 21st Century*, "Interdisciplinary Journal of Research and Development" 2023, Vol. 10, No. 1

24. Wallin M., *The New Public Diplomacy Imperative. America's Vital Need to Communicate Strategically*, New York: American Security Project, 2012
25. Wolfley J.K., *The Shape of Things to Come: Why the Pentagon Must Embrace Soft Power to Compete with China*, "Modern War Institute" 2021, <https://mwi.westpoint.edu/the-shape-of-things-to-come-why-the-pentagon-must-embrace-soft-power-to-compete-with-china/>
26. Zhang W., *China's cultural future: from soft power to comprehensive national power*, "International Journal of Cultural Policy" 2010, Vol. 16, No. 4

„Ante Portas – Security Studies"
2024, No 21
DOI: 10.33674/1202418

Vakhtang MAISAIA[1]
Georgia
Miranda MIKADZE[2]
Georgia

CBRN THREAT INFLUENCE ON INTERNATIONAL SECURITY – NEW DIMENSION OF SECURITY IN CONTEMPORARY GLOBAL POLITICS

Abstract: *In this way, during the Cold War, the political notion of security was extended, from referring primarily to matters related to defence and the military, such as the avoidance of military aggression, to dealing with economic, political, and societal matters, domestic as well as international. After the Cold War in post-Bipolarity period of time, the concept of security at global level cardinally changed and shifted and new types of challenges emerged, mainly of hybrid threats. The threats are increasingly transnational, like below – mentioned: Terrorism; Organized crime; Illegal trafficking; Illegal migration; Epidemic disease. Chemical, Biological, Radiological, and Nuclear threats present significant challenges to global security and pose grave risks to human life, infrastructure, and the environment. Identifying CBRN threats accurately and efficiently is crucial for effective prevention, preparedness, and response measures. This dissertation explores the theoretical concepts and modalities employed in identifying CBRN threats. By examining the theoretical foundations and practical methodologies, we aim to enhance our understanding of CBRN threat identification and contribute to the development of robust strategies for countering these threats. Identifying CBRN threats is a complex and multidimensional task that requires the integration of theoretical concepts and practical modalities. The theoretical concepts of securitization theory and risk assessment provide valuable frameworks for understanding the perception and evaluation of CBRN threats. Securitization theory allows us to examine the discourses and policies that shape the perception of these threats*

[1] Vakhtang Maisaia, PhD, Caucasus International University (Georgia); Józef Gołuchowski University of Applied Science (Poland), ORCID: 0000-0003-3674-3570.
[2] Miranda Mikadze, PhD, Caucasus International University (Georgia).

as security concerns, while risk assessment enables the prioritization of threats based on their severity and likelihood. The accessibility of CBRN materials by terrorist organizations and individuals has been facilitated by various factors, including advancements in technology, the globalization of information, and illicit black-market networks. The rapid dissemination of knowledge and the ease of communication have enabled the acquisition, production, and dissemination of CBRN materials by non-state actors, expanding the potential reach and impact of their terrorist activities. Furthermore, the transnational nature of CBRN terrorism transcends national borders, making it a global security concern that demands international cooperation, intelligence sharing, and coordinated efforts to identify, track, and neutralize potential threats. The emergence of chemical, biological, radiological, and nuclear (CBRN) terrorism poses a significant and complex challenge to global and national security, necessitating comprehensive understanding, effective countermeasures, and international cooperation. The increasing accessibility of CBRN materials and the transnational nature of terrorist organizations create a heightened risk of devastating CBRN attacks on a global scale. These attacks have the potential to cause mass human casualties, public health crises, destabilization of nations, and psychological trauma, thereby undermining societal resilience and challenging the ability of governments to protect their citizens. The vulnerability of critical infrastructure and essential services further compounds the complexity of addressing CBRN terrorism.

Keywords: *asymmetric challenges, CBRN threat, CBRN terrorism, "Securitization" theory, Cold War, global security, international cooperation, international security*

Introduction

Chemical, Biological, Radiological, and Nuclear (CBRN) threats present significant challenges to global security and pose grave risks to human life, infrastructure, and the environment. Identifying CBRN threats accurately and efficiently is crucial for effective prevention, preparedness, and response measures. This dissertation explores the theoretical concepts and modalities employed in identifying CBRN threats. By examining the theoretical foundations and practical methodologies, we aim to enhance our understanding of CBRN threat identification and contribute to the development of robust strategies for countering these threats. Identifying CBRN threats is a complex and multidimensional task that requires the integration of theoretical concepts and practical modalities. The theoretical concepts of securitization theory and risk assessment provide valuable frameworks for understanding the perception

and evaluation of CBRN threats. Securitization theory allows us to examine the discourses and policies that shape the perception of these threats as security concerns, while risk assessment enables the prioritization of threats based on their severity and likelihood.

Practical modalities such as intelligence gathering and analysis, sensor technologies, and data analytics with artificial intelligence play crucial roles in the identification of CBRN threats. Intelligence agencies collect and analyze information from various sources to identify potential threats, collaborating and sharing information to achieve a comprehensive understanding. Sensor technologies, including radiation detectors and chemical and biological sensors, provide real-time monitoring and early detection capabilities, enhancing threat identification. Data analytics and artificial intelligence algorithms analyze vast amounts of data, enabling the detection of patterns and anomalies that may indicate CBRN activities.

Similarly, data analytics and artificial intelligence (AI) have emerged as powerful tools in identifying CBRN threats. AI algorithms analyze vast amounts of data, detecting patterns, anomalies, and potential indicators of CBRN activities. Social media posts, online forums, and other digital sources are scrutinized to identify suspicious behavior or discussions related to CBRN threats. The integration of AI and data analytics augments human analysis, improving threat identification capabilities. However, ethical considerations, privacy concerns, and the need for human oversight must be addressed in deploying these technologies effectively.

National security serves as a critical modality for promoting stability within nations and across the globe. It encompasses a range of strategies, policies, and practices aimed at protecting a country's sovereignty, safeguarding its citizens, and maintaining social order. This dissertation explores the significance of national security as a key modality for promoting stability, highlighting its various dimensions and contributions to maintaining peace, order, and progress within societies.

New Security Dimension and CBRN Proliferation Dilemma

National security refers to the measures and actions taken by a government to protect its interests, values, and assets from internal and external threats. It encompasses dimensions such as military defense, intelligence gathering, economic stability, societal cohesion, and environmental resilience. Stability, on the other hand, refers to the condition of calm, order, and predictability within a nation. It encompasses social harmony, the rule of law, economic prosperity, and the absence of significant conflicts or threats that could disrupt the functioning of a society. National security plays a fundamental role in promoting stability by ensuring the protection of a nation's interests and the

well-being of its citizens. It serves as a shield against various threats that can destabilize a country, including terrorism, transnational crime, cyber-attacks, and internal unrest. By effectively addressing these threats, national security contributes to creating an environment of peace, order, and progress.

One of the primary objectives of national security is to safeguard a nation's sovereignty and territorial integrity. Sovereignty refers to the authority and independence of a state to govern itself without interference from external forces. National security measures aim to protect a country's territorial boundaries, prevent external aggression, and maintain military capabilities that act as a deterrent against potential threats. By ensuring sovereignty and territorial integrity, national security provides stability within a nation. It establishes a sense of security among citizens, as they are assured that their government has the capacity to defend and protect their homeland. This stability fosters trust, unity, and a sense of national identity, which are crucial for the functioning of a harmonious society.

National security is instrumental in maintaining internal order and social cohesion. It involves the protection of citizens from internal threats, such as terrorism, organized crime, civil unrest, and political instability[3]. Effective law enforcement mechanisms, intelligence networks, and counterterrorism measures contribute to ensuring the safety of citizens and preventing internal threats. Consequently, the Threat Identification Matrix provides a comprehensive analysis of the CBRN threat as a provision for national and global security challenges. By examining the strengths, weaknesses, opportunities, and threats related to the CBRN threat, decision-makers can develop strategies to mitigate risks, enhance preparedness, and respond effectively[4]. Addressing weaknesses through increased public awareness, resource allocation, and regulatory frameworks is crucial for strengthening defenses against CBRN threats. Leveraging opportunities, such as technological advancements, international cooperation, and public-private partnerships, can enhance response capabilities. Proactive measures are necessary to address emerging threats, counter the involvement of non-state actors, and manage the potential dual-use implications of advanced technologies. By considering the multifaceted nature of the CBRN threat, nations can develop comprehensive and integrated strategies to protect national and global security and mitigate the risks posed by CBRN incidents[5].

---

[3] N. Colletta, *Promoting Interim Stabilization in Fragile Settings: From Theory to Practice*, [in:] *Stabilization Operations, Security and Development, Routledge*, London 2013, p. 84.

[4] G. Frank, *CONTEST An Evaluation of Revisions to the UK Counter-Terrorism Strategy with a Special Focus on the CBRNE Threat (ARI)*, Real Institute Elcano, Madrid 2009, pp. 23-24.

[5] M. Kolencik, *Crime Scene Investigation in a CBRN Context*, ISEM Institute, New York 2021, p. 5.

The national security dilemma is a key modality for geopolitical instability, as it creates tensions between states seeking to protect their national interests. When one state makes a solid effort to enhance its security by increasing military capabilities, it simultaneously creates concerns for other nations who perceive this increase in power as a potential threat. This triggers a response from those nations to increase their military capabilities in the same way, finally leading to an escalating arms race dynamic that can ultimately lead to conflict. The book *The Security Dilemma: Fear, Cooperation and Trust in World Politics*, by Ken Booth and Nicholas J. Wheeler discusses how the national security dilemma creates tensions between states seeking to protect their national interests[6]. There is highlighted how the security dilemma at a national level can cause friction between countries trying to safeguard their interests while also underscoring importance building trust through diplomatic channels aimed at resolving disputes peaceably without resorting military force. Increasingly, it was recognized that international relations were not only about conflictual interactions between states but also about cooperative efforts to build a more stable and secure global community. Yet even as scholars looked for ways of promoting cooperation over competition among nations, they could not ignore the fact that geopolitical instability continued to be driven by an enduring feature of statecraft known as the security dilemma. This concept refers to a situation where one state's efforts to enhance its own security can inadvertently lead other states to feel threatened or insecure. The result is often a spiral of mistrust and tension as each side seeks to counterbalance perceived threats from others[7]. Any kind of conventional wars may also escalate into nuclear wars, through mistakes made in the frenetic atmosphere that often surrounds decision-makers in wartime situations. Danger of Nuclear Imbalances – there is no guarantee that vertical or horizontal nuclear proliferation will preserve the balance of power. Indeed, proliferation inevitably creates temporary imbalances which may then be exploited by aggressive states. After all, the Hiroshima and Nagasaki bombs were dropped to take advantage of precisely such a military imbalance. Usable nuclear weapons – Useable nuclear weapons. Developments in recent years have focused increasingly on the production of nuclear weapons that have a more precise and contained impact, making them useable. These tactical or battlefield nuclear weapons are no longer of symbolic importance alone. This has led to the theory of nuclear utilization target selection (NUTS), which rejects the logic of MAD in suggesting that it is possible for a limited nuclear exchange to occur. Irresponsible Nuclear Powers-Although the deterrent effect of nuclear weapons

[6] K. Booth, N. J. Wheeler, *The Security Dilemma: Fear, Cooperation and Trust in World Politics*, Palgrave Macmillan, New York 2008, pp. 43-44.
[7] *Ibidem*, p. 3.

worked during the bipolar first nuclear age, it is far less reliable in the less stable, multipolar circumstances of the second nuclear age. The possibility of a nuclear first strike relies on the existence of a political or military leadership that is not averse to risk-taking, or a leadership that, because of its values and beliefs, pursues symbolic violence as a method of total war in isolation from strategic considerations. The greatest concern is therefore that nuclear weapons may fall into the hands of military-based dictatorial regimes, or even terrorist organizations, which may have fewer scruples about using them[8].

CBRN Non-Proliferation and Its Geopolitical Implications: Black Sea Security Case-Study

The CBRN non-proliferation policy still remains as a key geostrategic provision in current international security system. The policy is determined by the implications of the NPT legal framework. The Nuclear Non-Proliferation Treaty (NPT) has played a role in decelerating nuclear proliferation, particularly among developed countries that possess the financial and technological capability to develop atomic weapons. Even when the specific provisions of the NPT were not fully implemented, bilateral treaties between the United States and the Soviet Union helped to reduce tension and promote caution, which may have ultimately helped to bring about the end of the Cold War.

The Black Sea region is strategically located between Europe and Asia, with several countries bordering its shores. Black Sea region has seen conflicts in recent years, including the annexation of Crimea by Russia in 2014 which raised serious concerns among other nations regarding territorial integrity/sovereignty issues impacting security across regions[9]. It is possible to identify a few key factors in terms of WMD proliferation threat from this regional perception. This area is interconnected and interchangeable with significant countries such as Russia, Turkey, Iran and NATO members like Romania, Bulgaria, and Ukraine. The Black Sea Region offers convenient access to transportation routes that connect different parts of the world. Unfortunately, this also means that there are significant risks associated with the smuggling and trafficking of advanced weapon technologies in the area. These threats must be taken seriously. Conflicts and escalations are frequent in this region. There is always a chance that incidents that escalate instability could lead to less effective countermeasures against WMD proliferation. In return, destructive outcomes and more tension could emerge within such

[8] A. Heywood, *Global Politics*, Palgrave Macmillan, Washington 2011, p. 72.
[9] M. Lancaster, *Troubled Waters – How Russia's War in Ukraine Changes Black Sea Security*, NATO PA Defence and Security Committee Report, Brussels 2023, pp. 3-4.

scenarios. We should mention that multiple states have varying capabilities and resources needed for monitoring and managing sensitive material and technologies linked to WMD developments. Lack of adequately enforced regulatory frameworks, suitable governance mechanisms, and limited collaboration among governments increase risks of unchecked power dynamics that could cause long-term destabilization of security across regions.

The terms, hybrid threats and hybrid warfare/war are sometimes used interchangeably, which is one of the reasons why the concepts can appear confusing. In addition, the concepts have been examined through many different disciplinary lenses: international relations, strategic studies, security studies, military studies, history and political science to name a few. This multidisciplinary analytical mosaic also blurs the picture of what the concept of Hybrid Threats actually entail. In this report the concept of Hybrid Threats is used as an umbrella concept, while hybrid warfare/war is part of the activity occurring under the Hybrid Threats umbrella. Frank Hoffman, often regarded as the father of the hybrid warfare concept, has said that his formulation draws on several schools of strategic thinking, making the concepts (hybrid warfare and Hybrid Threats) intellectual synergies. Indeed, the concepts have evolved over time. In Hoffman's concept, which focused on non-state actors like Hezbollah and Al-Qaida, their tactical and operational military activities are directed and coordinated within the main battle space to achieve synergistic effects, and to include tactics used by transnational networks like transnational organized crime and state actors. At the time Frank Hoffman started to use the "hybrid warfare" label, it was only one of many labels, which also included "New Wars", fourth-generation warfare and asymmetric warfare amongst others[10]. These were being used by analysts to conceptualize changes in contemporary warfare in line with the idea that war had become "substantially distinct" from older patterns of conflict. There are plenty other concepts that describe new forms of conflict/warfare: "surrogate warfare", "grey zone activity", "raiding", "unrestricted warfare" (origins Chinese), "reflexive control" (origins Russian), "new generation warfare"(origins Russian), "competition short of conflict", "active measures" (origins Russian), "non-linear warfare", "asymmetric warfare", "compound warfare" "ambiguous warfare", "political warfare", "information warfare", "cyber warfare". All of these are trying to describe very similar actions than the hybrid threats concept – interventions and operations targeted against states and institutions with multiple means. The concept of hybrid threats, however, is the only one that raises the issue of systemic vulnerabilities of democratic systems as particular targets and clearly argues for

[10] F. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington Virginia 2007, pp. 19-20.

comprehensive approach with civil – military cooperation from the very beginning.

The concept of hybrid threats has been increasingly debated in the academic circles. A recent Google Scholar search for the terms Hybrid Threats and Hybrid Warfare produced roughly 9,990 results, with most publications - some 6,970 - produced since 2014[11]. This is an indication that the hybrid threats concept is here to stay. But it does not mean that the concept is fully accepted and understood. In addition to the scientific and military context, the terms Hybrid Threats and hybrid warfare are also used in a political context which started with the annexation of Crimea in 2014. Political use of Hybrid Threats refers to manipulative, unwanted interference through a variety of tools: spread of disinformation/misinformation, creation of strong (but incorrect or only partially correct) historical narratives, election interference, cyber-attacks, economic leverage, to name just a few. Some of the activities may not even be illegal per se. Since Hybrid Threats are characterized as a combination of action, in academic analysis one action alone does not make the activity hybrid and in some cases even the threat aspect can be questioned. These actions and activities alone strictly speaking do not qualify them to be Hybrid Threats. However, they do belong to the landscape of Hybrid Threats. This means that as a political concept, Hybrid Threats can be seen as unacceptable foreign interference in sovereign states' internal affairs and space.

Hybrid Threat Perception and Strategic Stability at Global Level

Having considered how the strategic stability remains still unprecedented indication and only been determined in aegis of Cold War scenario. According to one of the definitions: Strategic Stability – is defined as a characteristic of deterrence based on mutual assured destruction and is measured largely in terms of the potential vulnerability of strategic force components, notably land-based missiles[12]. In shifting drifts of contemporary international security system, strategic stability is being affiliated with new threat – hybrid threat modality. The one is shaping and making its contribution of true identity of the system.

The hybrid threats is a broad overarching concept that includes many types of activity: interference, influence, operations, campaigns and warfare/war. All of these activities can be seen as unwelcome interventions of one sort or another to a country's internal space. We need to keep in mind that the term

[11] O. Fridman, *Russian Hybrid Warfare: Resurgence and Politicization*, Oxford University Press, London 2018, pp. 23-25.

[12] J. Streinbrunen, *National Security and the Concept of Strategic Stability*, "Journal of Conflict Resolution" 1978, Vol. 22, No. 3, p. 411.

Hybrid Threats is a Western concept used to discuss a security dilemma that states face which either have a democratic state system or are in the democratization phase. This is how the context is framed in most of the Western literature relating to Hybrid Threats. The concept has penetrated to Russian and Chinese writings today, but they did not use the name "Hybrid Threats/Hybrid warfare" before it was widely discussed in the Western security debate. The characterization of Hybrid Warfare can be found in both the Russian and the Chinese literature. They claim that Western countries are using hybrid warfare against them. This claim is often done without giving a context, with strong support for the state's official line. The references used from Western literature ignore the fact that the used references describe the action by a hostile actor against the Western countries. This fact is not mentioned.

The various academic sources identified three phases with different intensity of action and nature of the threat. This means that an escalation potential exists. These phases are explained later in this document. The activities and phases follow a rather conventional understanding, with slight modifications, of how a threat is constructed and how it might escalate. The activities and phases in themselves do not characterize a threat as hybrid, but they belong to the landscape of Hybrid Threats and are therefore also an integral part of understanding the nature of the threat element of Hybrid Threats. A major ongoing debate concerns old versus new ways of exerting interference and influence[13]. In this debate both, those that argue that there is nothing new relating to Hybrid Threats and those that see Hybrid Threats as a fully new security challenge, have a point. As Mikael Wigell, senior researcher at the Finnish Institute of International Affairs, has argued, "many scholars and analysts contest the utility of the hybrid label, criticizing it for conveying little that is new, for being imprecise, or outright misleading. The author called hybrid methods are used alongside more usual deterrence policies" coupled with the term 'warfare', critics warn, there is the danger of unnecessarily militarizing the language of international politics with potentially dangerous consequences"[14]. What this boils down to is bearing in mind that from the point of view of military-strategic thought, the analytical utility of the "hybrid warfare" concept is contested and, as a tool to analyze military capabilities, its usefulness is very limited.

In recent international politics remains very unstable and after switching again world order structure and percussion occurred in stability of the ongoing international security system. As it is perceived main missions of the

[13] W. Murray, P. Mansoor, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, London 2012, pp. 56.

[14] M. Wigell, *Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy*, "International Affairs" 2019, Vol. 95, Issue 2, p. 256.

international security as structural element of the global politics remain in avoiding wars and military conflicts and perceives of examining power capability. The definition "International Security" is being affiliated with the UN Charter.

Threat assessment criteria is being considered as the most prevalent academic instrument in reaching true realms of logics of international relations. In the 21st century threat identification has determined and transformed into concrete systematic modality. Having considering the "Copenhagen School" securitization concept where there are five ring of security provisions that are enlisted in the following way:

- Political Security;
- Military Security;
- Economic Security;
- Society Security;
- Environment Security.

Therefore with enumerating "five ring" provision in 20-21st century's two academic sub-fields in international relations have been emerged. Namely, Strategic and Security studies as a whole, represented the most important contribution to the research of security issues in aegis of the political science. Even today, some authors consider them to be the only real research platform in the area of research of security[15]. In that manner is important of true classification of threat identification that could be clarified in manner of: threat-challenge-risk. However, the classification is still plausible and general and yet to have confirmed in academic and analytical methodology frame. Nevertheless, there are two types of the threat that is already identified but in general way – symmetric and asymmetric threats[16].

Namely, military security dimension is more applicable for analyzing situation and importance of the region in aegis of international politics. Treating the region from the military perspective is necessary introduce a jargon "Geostrategic Gateway" – space or area vitally important from global security and military perspectives, like "southern limited flank" in aegis of the CFE Treaty of Istanbul OSCE Summit[17]. Relatively the Black Sea regional security is referred as "Geostrategic Gateway" mainly due to contemporary "New Cold

[15] R. Ondrejscak, *Introduction to Security Studies*, Centre for European and North Atlantic Affairs, Bratislava 2014, pp. 12-14.

[16] E. Beraia, *The U.S. Foreign Policy Priorities in the Post-Cold War Period (1990-2016): Georgia's Case from Transnational Challenges (Including Migration) towards Enhancing Institutional Transformation*, Ph.D. thesis at International Black Sea University (IBSU), American Studies Program, Tbilisi, Georgia 2017, pp. 67-68.

[17] Author personal definition.

War" provision where a coercive competition between NATO and Russia for getting dominance over the Black Sea region.

Due to the strain relations between the West and Russia, from one standpoint an economic war between EU/USA and Russia via sanction policy level and a military confrontation between NATO and Russia via demonstration "military muscles" between competing forces. In that scope, mainly NATO-Russia military confrontation one of the dangerous "combat zone" is sought to be the Black Sea Basin and its littoral territories which is labeled as the "Black Sea Security Dimension". The flawed geostrategic situation in the area is making possible to deteriorate geostrategic environment in the area further on and the indication derives from those actions taken by the Russian Federation incumbent authority.

Black Sea Regional Security Case-Study: as it is known, on July 27th 2015 a new naval doctrine was declared and later approved by the President of the Russian Federation. This document has identified new version or interpretation of the military doctrine that was approved by the National Security Council in December of 2015. The naval doctrine has identified strategic areas and basins, such as the Artic and the so-called "Atlantic" direction, which includes the Black Sea basin. The doctrine also undermines the role of the fleet (both military and civilian), the shipbuilding industry, harbors and rigging infrastructure as priorities for the further development of Russia's naval economy. How is seen based on these documents, Russia is trying position itself as a great power with ability to increase its military capability on the Caspian-Black-Mediterranean Seas axis. The center of this axis is the Black Sea, a basin from which NATO risks being excluded. The Russian policy-makers seek to regain its nation's great power status-quo with domination in the basin with controlling three key points: Crimea, the mouths of the Danube and the Bosporus. Having considered the latest events, Russia has partially achieved the strategic goals – first occupied and then annexed the Crimea and reinforced military positions and capabilities in the peninsula, with creation of so-called "Mediterranean Task Force' within the Black Sea Fleet and detachment of combat ships and boats for the Mediterranean Sea and the Gulf region, Russia pursued getting its control Bosporus (the Task Force was reinforced by the nuclear carried submarine "Rostov-on-Don", which sailed from Novorosiisk to join the Force and equipped with newest strategic weaponry system "Kalibr" missiles)[18]. With this reinforcement naval forces, Russia is seeking to get under the control the third pillar – the mouth of Danube. However, in order to more reinforce its presence in the Black Sea

[18] V. Maisaia, M. Beselia, *Asymmetrical Warfare Strategy and Its Implications to the Black Sea Regional Security in 21st Century: Non-State Aggressive Actors and Terrorism*, "Ante Portas – Security Studies" 2020, No. 2 (15), p. 73.

basin, the Russian authority announced that 30 new ships are to be supplied to the Black Sea Fleet, including six new frigates, six new submarines and other smaller vessels for naval landing. In addition to that the Black Sea Fleet will be reinforced its anti-access strategy (A2/AD) against NATO forces. Taking together all these factors, and precise attention to the regional security environment, if the Russian government completes its missions in that way how it prescribed in the naval doctrine, the Black Sea Fleet will have full control over the Black Sea by 2020. In that retrospective provision, the military balance at present time between the NATO and Russian forces decreased in proportion of 2:1 in favor to the NATO ones but in that reinforced conditions by 2020 the balance will be absolutely opposite in the same proportion but in Russia's favour. In that configuration, Georgia is in dangerous positions due to its littoral space and its unfrozen sea ports that Russia needs very badly[19]. Hence, Georgia is to be perceived new aggressive steps from the Russian authority after the Parliamentary elections, namely toward the ports directions. Hence, the Georgian government and society have to very attentive toward any provocations spurred from the Russian side.

Above-mentioned case are indicated on various approaches from conventional misbalance effect on strategic stability provisions and CBRN threat perception implications on contemporary international security environment. It is vivid scenario why it makes frangibility of security identification causing real risk and threat to strategic stability processes.

Conclusion

At time being, security has traced into global dimension determined by the Globalization phenomenon and acceleration of integration processes. Due to massive effect of threats and risks for Global Politics, a new definition of Global Security emerged in vocabularies of international relations and secudirt studies. According to them, Global Security – is a security model that is implemented by the international and intergovernmental organizations and based on principles of international law principles and norms and backed on this background, the states, as international political actors, are obliged to comply with these ones, by keeping sovereignty untouchable and in case of its of violation take offshoot[20]. Meanwile, the global threat could be emanated not only from states but also from such subjects yet to be identified as an international actors and even international law is uselness in eradication ones and their behaves, like "DAESH" or even COVID-19 virus. Such precedents need more precise and deliberate approaches and analyses. Hence adaptation of

[19] *Ibidem*, pp. 74-75.

[20] Author personal definition and term identification.

the field of study in Georgia and namely in CIU will promote development of research internationalization tool of the field and Georgia will take part in promotion of the academic field sophistication.

The modern international relations and security environment is characterized by many threats and challenges. This annual is a companion of the 21st century. Along with technological development, the rise of aggressive non-state groups, extremist forces, and individual terrorist groups have created many threats. Consequently, asymmetric threats are becoming more and more common. Important among them are threats from bioterrorism, which can lead to catastrophic consequences. It should be noted here that the risks and dangers arising from biological warfare pose significant threats and challenges to the international community and the entire world. Biological warfare and bioterrorism can destroy a large number of people and the biosphere in the shortest time and with minimal costs. All this is really a serious problem for global security. Based on all of this, it is necessary to actively develop international cooperation mechanisms to ensure a modern biosafety system. In the light of modern threats and challenges, it is very important to develop scientific research in the field of prevention and control of biological threats. Also, the most important issue is the activation of cooperation between states, regional and international organizations regarding the prohibition and control of biological weapons and the fulfillment of obligations.

One of the main events in modern international political developments is the military dimension of global security. Any state has at least two obligations towards its citizens: to ensure their *security* and create conditions for any citizen to increase their well-being (both material and spiritual). Security covers many aspects of public life and implies the neutralization of completely different types of dangers. This may refer to the physical rescue of a citizen and the protection of their life from a bandit attack or, say, protection from the encroachment of their life by the military force of another country. At the same time, the state must be able to protect its own institutions and the inviolability of the borders of the country, which is primarily carried out by using the military forces and capabilities of the country. In this regard, it is important to discuss a phenomenon in this context, which is an essential component of the security of a country, that is - military security. The term "military security" itself means the ability of a state to defend or prevent military aggression from another country (or countries)[21].

[21] V. Maisaia, A. Guchua, *NATO and Non-State Violent Religious Actors ("DAESH", "Al-Qaida" and "Taliban") – The Fourth War Generation Strategy and Geopolitical Aspects of Its Regional and National Security (2010-2019),* Caucasus International University (CIU), Tbilisi 2020, pp. 10-12.

One of the important new dimensions of military security, which determines global and regional security conditions in the military-political context, is the term: “Geostrategic environment”. Under the auspices of the mentioned term, it is meant the combination of political, economic, socio-technological, and military factors that have a negative impact on the military security of the country. The components of the geostrategic environment are represented by three important things:

- Geopolitical transformation - the end of US hegemony and the development of a multipolar world order and the emergence of non-state actors or new centers of influence in it;
- Military-technical confrontation - considerable lag in the military potential of the Georgian Defense Forces in the field of offensive weapons and conventional weapons compared to neighboring countries;
- The new wave of military confrontation between the states, "arms race" - the development of the new "Cold War" and its epicenter in the Black Sea area.

It is also worth noting the fact that the modern geostrategic environment at the global level, which clearly experiences high turbulence, was formed after passing through certain evolutionary phases, within which the modern military strategic culture and art were formed.

BIBLIOGRAPHY:

Books and articles:

1. Beraia E., *The U.S. Foreign Policy Priorities in the Post-Cold War Period (1990-2016): Georgia’s Case from Transnational Challenges (Including Migration) towards Enhancing Institutional Transformation*, Ph.D. thesis at International Black Sea University (IBSU), American Studies Program, Tbilisi, Georgia 2017
2. Booth K., Wheeler N. J., *The Security Dilemma: Fear, Cooperation and Trust in World Politics*, Palgrave Macmillan, New York 2008
3. Buzan B., Waever O. De Wilde J., *Security, A New Framework For Analysis*, Lynne Reinner Publishers, London 1998
4. Buzan B, Kelstrup M., Lemaitre P., Tromer E., Waever O., *The European Security Order Recast: Scenarious for the Post-Cold War Era*, Centre for Peace and Conflict Research, London 1991
5. Colletta N., *Promoting Interim Stabilization in Fragile Settings: From Theory to Practice*, [in:] *Stabilization Operations, Security and Development*, Routledge, London 2013
6. Chifu I., Sauliuc A., Nedea B., *Energy Security Strategies in the Wider Black Sea Region*, Editura Curtea Veche, Bucharest 2010

7. Dannreuther R., *International Security: The Contemporary Agenda*, second edition, Polity Press, UK 2017
8. Heywood A., *Global Politics*, Palgrave Macmillan, Washington 2011
9. Hoffman F., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington, Virginia 2007
10. Fridman O., *Russian Hybrid Warfare: Resurgence and Politicization*, Oxford University Press, London 2018
11. Frank G., *CONTEST "An Evaluation of Revisions to the UK Counter-Terrorism Strategy with a Special Focus on the CBRNE Threat (ARI)"*, Real Institute Elcano, Madrid 2009
12. Kolencik M., *Crime Scene Investigation in a CBRN Context* ISEM Institute, New York 2021
13. Lancaster M., *Troubled Waters – How Russia's War in Ukraine Changes Black Sea Security*, NATO PA Defence and Security Committee Report, Brussels 2023
14. Murray W., Mansoor P., *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, London 2012
15. Maisaia V., Beselia M., *Asymmetrical Warfare Strategy and Its Implications to the Black Sea Regional Security in 21st Century: Non-State Aggressive Actors and Terrorism*, "Ante Portas – Security Studies" 2020, No. 2 (15)
16. Maisaia V., Guchua A., *NATO and Non-State Violent Religious Actors ("DAESH", "Al-Qaida" and "Taliban") – The Fourth War Generation Strategy and Geopolitical Aspects of Its Regional and National Security (2010-2019)*, Caucasus International University (CIU), Tbilisi 2020
17. "Munich Security Report 2018" – Munich Security Conference, Munich 2018
18. Ondrejscak R., *Introduction to Security Studies*, Centre for European and North Atlantic Affairs, Bratislava 2014
19. Streinbrunen J., *National Security and the Conflict of Strategic Stability*, "Journal of Conflict Resolution" 1978, Vol. 22, No. 3
20. Wigell M., *Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy*, "International Affairs" 2019, Volume 95, Issue 2

Electronic Literature Source:

1. Abrams A., *Here's What We Know So Far About Russia's 2016 Meddling* published in "Times" on April 18, 2019, <https://time.com/5565991/russia-influence-2016-election/>
2. Barnes J., *Russian Interference in 2020 Included Influencing Trump Associates, Report Says*, published in "The New York Times" on March

16, 2021, <https://www.nytimes.com/2021/03/16/us/politics/election-interference-russia-2020-assessment.html>
3. Young K., *Shows How Russia's Election Interference Has Gotten More Brazen*, published in Special Report by Brennan Centre for Justice on March 5, 2022, <https://www.brennancenter.org/our-work/analysis-opinion/new-evidence-shows-how-russias-election-interference-has-gotten-more>
4. *The UN Charter, Chapter One: Purposes and Principles*, https://www.un.org/en/sections/un-charter/chapter-i/index.html
5. NATO parliamentary Assembly, Defense and Security Committee (DSC), *Troubled Waters-How Russia's War in Ukraine Changes Black Sea Security*, 2 May 2023. P. 4 <https://tinyurl.com/2fcx62w2>

„Ante Portas – Security Studies”
2024, No. 21
DOI: 10.33674/1202419

Thornike ZEDELASHVILI[1]
Georgia
Alika GUCHUA[2]
Georgia

ARTIFICIAL INTELLIGENCE AND WEAPONS OF MASS DESTRUCTION

Abstract: *There is considerable evidence in the modern history of warfare that when tensions between states are high, decision makers are more likely to seek detours or shortcuts to war to avoid great losses and costs. Accidental wars and unintentional escalations are actually relatively rare, despite fears and some signals of rising tensions. It is this type of warfare that is a major source of concern for many states, especially when combined with high-risk weapons systems or systems with the potential for mass destruction. The purpose of the article is to determine the role of artificial intelligence in the policy of non-proliferation of weapons of mass destruction. Among the most dramatic risks of escalation through the use of artificial intelligence is nuclear conflict. This topic has received significant and increasing political attention and research in recent years, driven by two main factors. The first is the tremendous progress that has been made in the field of artificial intelligence, especially machine learning. Such advances may provide an opportunity to improve early warning and decision support systems, or may contribute to improved targeting data. A second related reason is that competitive pressures to implement artificial intelligence in a different area amid the discourse of the "global race" have the potential to accelerate the adoption of artificial intelligence in the nuclear architecture. With its implementation, new risks of accidents, unforeseen escalation and vulnerability may arise. Artificial intelligence also expands the range of attack options that an attacker can take advantage of, including using cyber-attacks and information operations. The objective of the article is to*

[1] Thornike Zedelashvili, PhD, Caucasus International University (Georgia), ORCID: 0000-0003-2630-1779, email: thomaszedelashvili@gmail.com
[2] Alika Guchua, PhD, Caucasus International University (Georgia), ORCID: 0000-0003-0347-9574, email: alika_guchua@ciu.edu.ge

determine with the development of artificial intelligence, what role it will play in the non-proliferation of weapons of mass destruction or vice versa.

Keywords: *nuclear weapons, artificial intelligence, weapons of mass destruction, strategy, war, threat, automation, global race.*

Introduction

Interest in automating nuclear deterrence has long been on the agenda of the United States and the Soviet Union, but technology limitations have also made it clear that decisions about nuclear strikes cannot be delegated to an automated system. In short, humans must remain in the loop to analyze information, verify technical functions, and make the decision to launch a nuclear weapon, because there is a risk that automated technologies will for some reason provide the wrong information to the center. The capabilities of artificial intelligence (AI) have rapidly advanced over the last ten years. Developments in machine learning (ML) techniques, which enable computer systems to "learn" from data to carry out activities that would otherwise need human intellect, have fueled this process[3]. State interest in using AI systems for military objectives has grown as a result of advancements in fields including computer vision, natural language processing, robotics, and autonomous systems. For decades, the military has used autonomous weapons such as mines, torpedoes, and heat-guided missiles that operate based on simple reactive feedback without human control. However, artificial intelligence (AI) has now entered the arena of weapons design[4].

Artificial intelligence (AI) is a catalyst for many trends that increase the salience of nuclear, biological or chemical weapons of mass destruction (WMD)[5]. The creation or production of WMD or precursor technologies can be aided and expedited by AI. Those without the knowledge to create hazardous compounds or fissile materials can develop WMD capabilities with AI's help. The proliferation of AI itself is a concern. Since it's an intangible technology, it spreads readily and is hard to stop with supply-side measures like export restrictions. There are worries about increased dangers of accidental or

[3] V. Chernavskikh, *Nuclear weapons and artificial intelligence: technological promises and practical realities*, 2024, <https://www.sipri.org/sites/default/files/2024-09/bp2409_ai-nuclear.pdf> (10.10.2024).

[4] C. Caruso, *The Risks of Artificial Intelligence in Weapons Design*, Harvard College 2024, <https://hms.harvard.edu/news/risks-artificial-intelligence-weapons-design> (11.10.2024).

[5] O. Meier, *The fast and the deadly: When Artificial Intelligence meets Weapons of Mass Destruction*, 2024, <https://europeanleadershipnetwork.org/commentary/the-fast-and-the-deadly-when-artificial-intelligence-meets-weapons-of-mass-destruction/> (14.10.2024).

deliberate use of nuclear weapons, decreased crises stability, and new arms races at the nexus of AI and nuclear weapons.

In general, the nuclear industry has historically been conservative and reluctant to integrate digital technologies for the obvious reasons of reducing the risk of new system vulnerabilities. However, while many legacy systems are considered analogous, there are clear signs from several nuclear powers, including the United States and the Russian Federation, that they are seeking to modernize their nuclear architecture.

Artificial Intelligence has the potential to enhance the intelligence and autonomy of any military system, be it cyber, conventional, or nuclear. However, a number of drawbacks in AI systems make their possible application challenging from a security, legal, and ethical standpoint[6]. Although the status of AI integration in nuclear command, control and communications (NC3) systems, for example, cannot be fully assessed because the information is not publicly disclosed, the growing literature on the possible uses of ML shows clear areas of opportunity.

The use of artificial intelligence in nuclear deterrence architecture may be particularly attractive for early warning systems. For example, computer vision algorithms can be used to detect unusual movements of troops or equipment. AI can be used to improve speed and accuracy by processing large amounts of data more efficiently and as a means of autonomously classifying enemy behavior with remote sensors. This will also allow for more accurate anomaly detection. Significant progress has been made in this field in recent years, and for example, a study published in 2022 demonstrated the effectiveness of using high-precision neural networks to improve target detection in radar signals.

While AI could theoretically make deterrence more effective, there remains a risk that the system may misperceive escalation, or perceived threat, because human actions are misperceived. The imperfect data used in complex systems means that decisions based on such data can increase the alarm status.

In the area of nuclear command and control, nuclear-weapon states are likely to be slow to adopt AI simply because the technology is so vulnerable and unpredictable. However, there are more reasons why ML (machine learning) could affect the delivery of nuclear weapons, including using autonomous systems such as unmanned aerial vehicles.

They provide more flexibility than nuclear ICBMs (Intercontinental ballistic missiles), better avoid obstacles and have the ability to cover larger areas. However, the use of unmanned systems to deliver nuclear weapons poses a

[6] V. Boulanin, *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, Vol. I Euro-Atlantic Perspectives, Stockholm International Peace Research Institute 2019, p. 4, <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf> (16.10.2024).

threat to human control. There are different regional views on the feasibility and acceptability of their use, but the problem remains that states that feel relatively vulnerable in their nuclear arsenals may assess the risks and benefits differently.

The impact of artificial intelligence on nuclear risks is not only related to the use of AI technologies in nuclear architecture. Advances in artificial intelligence and its capabilities (such as remote sensing and autonomy) can improve the speed, accuracy, lethality, and survivability of conventional weapons. This opens up new avenues for escalation, both horizontal and vertical inadvertent escalation. Conventional forces can be used more effectively against enemy nuclear forces. Or some states may perceive advances in conventional weapons systems as a threat to their future second-strike capabilities. This could lead to a doctrinal shift that could legitimize the limited use of nuclear weapons by some states against what they perceive as more powerful conventional adversaries.

Even before the deployment of weapons in different areas of the country, AI can perceive a violation of strategic stability as the cause of a new threat. Government investments in AI can create a sense of vulnerability in the adversary, which can lead to further instability and destabilizing actions. At the same time, attackers may significantly underestimate the true extent of AI capabilities or their use, thereby creating additional pressure.

Proliferation Risks - AI can facilitate the proliferation of new weapons, for example by converging with other fields of science and technology, or by making existing weapons systems more lethal and autonomous. Therefore, the use of AI has become more attractive in order to spread new weapons and implement them in various fields. Ultimately, though, in an era of renewed great power tensions, the major military countries will be wary of regulating too soon, for fear of stifling innovation and constraining themselves unnecessarily[7].

Convergence risks - biosecurity and chemical weapons

The convergence of artificial intelligence and biotechnology is producing novel threats which pose an existential risk both to specific demographic groups and the population at large[8]. The convergence of artificial intelligence, biology and chemistry has created opportunities for medical breakthroughs and

[7] S. Cleobury, *Artificial Intelligence and Arms Control – How and Where to Have the Discussion,* Geneva Centre for Security Policy 2023, <https://www.gcsp.ch/publications/artificial-intelligence-and-arms-control-how-and-where-have-discussion> (21.10.2024).

[8] R. Donaldson, *Sounding the alarm on AI-enhanced bioweapons*, European Leadership Network 2024, <https://europeanleadershipnetwork.org/commentary/sounding-the-alarm-on-ai-enhanced-bioweapons/> (23.10.2024).

drug discovery, but it also perfectly illustrates the risks of dual use. For example, a class of LLMs (Large language models) called chemical language models (CLMs) are used to discover new treatments and, among other things, to predict potential drug molecules that target specific disease-causing proteins. AI language models can be used to design new proteins. (e.g. ProtGPT2) and while potentially contributing to disease control solutions, such applications may create opportunities for misuse. In recent years, researchers and political communities have focused on the risks of misuse of artificial intelligence in biotechnology. One critical risk concerns the proliferation of biochemical weapons, although the risks are more varied and have several levels of complexity.

Expanding the influence of artificial intelligence to achieve nuclear stability

The potential impact of AI technologies and systems on nuclear defense and stability extends beyond advances in cyber threats and the proposed use of AI-based systems for nuclear attack early warning systems. Unmanned ships with autonomous navigation capabilities equipped with artificial intelligence systems are expected to have a significant impact on nuclear deterrence based on SLBMs (Submarine-launched ballistic missiles). Autonomous unmanned ships are being developed as new elements of undersea warfare, similar types of unmanned ships are a new word in the art of warfare. Their main purpose is to detect submarines, including those out of port, and follow them for long periods of time, and if necessary, attack and destroy them.

In recent times, it is significant to generate synthetic data called deep fakes, which are often used to make imitation videos of political leaders. These increasingly realistic and seductive videos can create misconceptions about the personalities, behavior, political positions and actions of the political leaders depicted. Deeply faked videos of current and former nuclear power leaders such as Barack Obama, Donald Trump, Joe Biden and Vladimir Putin have been widely circulated, raising doubts about their consistency and rationality.

Technological progress has brought about the emergence of machines that have the capacity to take human lives without human control. These represent an unprecedented threat to humankind[9]. The race to militarize AI was initially driven by the emergence of autonomous weapon systems (AWS). These are weapon systems with artificial intelligence that select and direct force to attack targets without human intervention. Examples include mobile munitions and

[9] B. Dresp-Langley, *The weaponization of artificial intelligence: What the public needs to be aware of*, National Library of Medicine, <https://pmc.ncbi.nlm.nih.gov/articles/PMC10030838/> (25.10.2024).

autonomous drones. Mobile munitions are flown in a designated area to sink or destroy certain targets, after they are activated, further human intervention is impossible. But using AI for nuclear command, control, and communications might also lead to arms races or make it more likely that states will use nuclear weapons in an emergency, whether on purpose or by mistake. AI can play a role in this process without being directly related to nuclear launchers. For example, it might advise humans on escalation-related issues. By enabling quicker real-time analysis of systems and data and improving situational awareness, artificial intelligence (AI) holds promise for supporting decision-makers. However, this could shorten the time needed to make decisions and result in more tensions, misunderstandings, and miscommunications – including between states that possess nuclear weapons[10].

The Turkish STM Kargu-2 unmanned aerial vehicle was used in an autonomous attack mode against Haftar-linked forces during the second Libyan civil war. The variety of uses of existing autonomous weapons is constantly expanding.

AWS raises serious concerns regarding the protection of international human rights (IHL - International humanitarian law) in conventional conflicts. In addition, AWS has the potential to give users of conventional military technology a greater advantage in the conventional weapons space. In this regard, it has been argued that if the AMC upsets the conventional balance, and therefore a nuclear-armed adversary may be incentivized to threaten the use of nuclear weapons in order to avoid military defeat of its adversary.

In the Soviet Union, when they thought that their country was not as powerful as the United States of America, the system "Perimeter" was created - in the West it is called "Dead Hand". If for some reasons the highest authorities are removed from the pile, the emergency system of computers requires the response of the heads of state. If it doesn't get a response, sensors that detect radiation, shock waves and radio-electronic pulses will prompt the system to deploy special signal missiles that will launch from a height and from there transmit a signal to all surviving elements of Russia's nuclear triad. That is, even if the three heads of the country - the president, the chief of the general staff and the minister of defense - die, the system will still retaliate.

At the beginning of the 90s, they talked about shutting down this system. But recently, the commander of the Russian Strategic Missile Forces, General Karakaev, said that it is modernized and ready for combat. If a missile is detected from the US, there will be a retaliatory strike from Russian territory. These rockets may meet each other in mid-air, continue their flight and

[10] *Proceed with Caution: Artificial Intelligence in Weapon Systems, AI in Weapon Systems Committee*, Report of Session 2023-2024, Published by the Authority of the House of Lords, p. 51, <https://publications.parliament.uk/pa/ld5804/ldselect/ldaiwe/16/16.pdf> (26.10.2024).

eventually crash at their destination. It will be mutual destruction. The situation is the same in America, but the US is considering a preventive strike as well. The Russian military elite is talking about reflecting this in the Russian military doctrine[11].

In discussing these issues, it is important to focus on false alarm cases of missile attack - situations when the world was on the brink of global nuclear war. Today, apart from the Caribbean crisis, 4 such cases are known. Two of these are related to the Soviet missile attack warning system and two to the American early warning system[12].

First case

The first time at 9:00 a.m. on November 9, 1979, on the computers of the North American Aerospace Defense Command (NORAD) (located in the Cheyenne Mountains Bunker), the Pentagon's National Command Center and the Reserve Command Center at Fort Richey saw a message that the Soviet the Union launched a massive nuclear strike to destroy the control system and US nuclear forces have collapsed. High-ranking military personnel were immediately announced from all three points and took part in the emergency meeting. An order was sent to the special equipment "Minuteman" to be ready for launch. Alerting the entire air defense system, at least ten aircraft immediately took to the skies, as well as the air defense of the president's plane, although without the president himself. After receiving the message about the attack, a few minutes after checking the data on the satellites located around the US territory, it turned out that there were no signs of an attack on any of them, so the alarm was canceled. Later it turned out that the reason for providing false information was a computer game that was mistakenly uploaded to the computer of a soldier on duty.

Second case

On June 3, 1980, the US military again received a warning of a missile attack. At first the launchers were mobilized and the crew took their places in the bombers, but this time the computers did not give an accurate and clear picture of the attack as the first time. Instead, the screen showed constantly changing numbers of missiles launched. Also, these numbers did not always match at different control points. Many officers did not take this incident as

---

[11] *What are the rules for launching nuclear weapons?*, Tbilisi 2022, p. 1, <https://www.radiotavisupleba.ge/a/31735977.html> (28.10.2024).

[12] *Four cases when the world was on the verge of nuclear war*, Tbilisi 2019, <https://geostate.ge> (05.11.2024).

seriously as the previous one, but a state of emergency was still declared to assess the likelihood of an attack being real. The information from the satellite and radar was checked again. And again, not a single system claimed the fact of a missile attack. It was later discovered that the reason for this was a malfunction of a single circuit in the computer, which reflected the random numbers of the missiles launched[13].

The third case

September 26, 1983 might have been not only the most difficult date in world history, but also radically changed the future life of the world, if not for the sound judgment and courageous decision of a Soviet officer who saved the world from a nuclear disaster[14]. Lt. Col. Stanislav Petrov's decision to save humanity from nuclear war in 1983 is a lesson to humanity about the risks posed by technological advancement and the special efforts to make such advancements in the war arena[15]. In 1983, the Cold War between the United States and the Soviet Union reached its peak, less than a month after the tragedy when the Soviet Union shot down a South Korean passenger Boeing 747 near Sakhalin, which killed 269 innocent people, this is what Stanislav Petrov first thought that maybe this new to become a pretext for war. On September 26, 1983 (according to other data, in July), the satellite echelon of the Soviet system, put on combat duty, announced the American missile attack. The satellites, which were located in an elliptical orbit, observed the American missile bases from the angle that they were at the edge of the visible disk of the Earth. This made it possible to detect the rockets on the launch pad against the background of dark space, thus determining the fact of the launch of the rockets, by infrared radiation that works on the rocket engine. Such a configuration was chosen to reduce the glare of the satellite's sensors, which was reflected by the clouds or by the sun's rays on the snow. However, on this day, after noon, the satellite, the area of American missile bases, and the sun came into such an arrangement that the sun's rays reflected strongly from the clouds, which were located very high. The satellite reported the launch of several rockets from the American continent. However, radar observations did not confirm this, as the missiles were located too far away[16].

---

[13] *Four cases when the world was on the verge of nuclear war*, Tbilisi 2019, p. 1, <https://geostate.ge> (08.11.2024).

[14] *Who is the man who saved the world from a nuclear disaster*, Tbilisi 2021, p. 1, <https://intermedia.ge> (10.11.2024).

[15] *Ibidem*.

[16] *Four cases when the world was on the verge of nuclear war*, Tbilisi 2019, p. 1, <https://geostate.ge> (12.11.2024).

Lieutenant Colonel Stanislav Petrov was on duty at the control panel at the time, after analyzing the information (the missile "launch" was made from only one point and consisted of several intercontinental ballistic missiles) and based on the reports of the "visuals" (officers who monitored the air and space on video control screens and no missile activity was detected), Lt. Col. Petrov decided that this was a false alarm received from the system. No, and upon receiving information about the threat, the leadership of the Soviet Union had to be informed about the alleged American missile attack - they were the General Secretary of the Communist Party of the Soviet Union (Yuri Andropov), the Minister of Defense (Dmitry Ustonov) and the Chief of the General Staff of the Armed Forces of the Missile Forces. (Yuri Votintsev). Stanislav Petrov's heroism can be appreciated by the fact that the Soviet military discipline provided for unspoken obedience to superiors and unconditional execution of orders, without any interpretation of his own.

This incident highlights the importance of human power alongside the work of artificial intelligence. The US National Security Commission on Artificial Intelligence (NSCAI) recommends that it not be entrusted with nuclear weapons and that humans take the reins, while there are additional risks posed by AI's inherent vulnerabilities and special needs for information processing.

The fourth case

Early in the morning of February 25, 1995, a Norwegian scientist, with the help of the Americans, launched the most powerful weather missile ever from Anoia, off the coast of Norway. The purpose of the rocket was to study the North Sea, in the construction of which the first stage American tactical missile "Honest John" was used. It flew at an altitude of 580 kilometers. During observation, the flight trajectory of the missile was found to be suitable for the American missile «TRAIDENT» D-5, which was launched from the submarine. Such a missile could be used for a high nuclear explosion that would disable Russian warning radars. An explosion at such a height was seen as a massive nuclear attack by the Americans. The launch of the Norwegian missile threatened the world with a retaliatory nuclear strike from Russia against the USA. The next day, President Boris Yeltsin announced that he had activated his "nuclear suitcase" for the first time for emergency contact with the militants to discuss the situation. In addition, in the 1990s, the Russian space echelon operated at full capacity to provide quality detection of enemy missile launches. With all this, according to Viktor Barantz's memoirs, the launch of the Norwegian missile was "news" only for the Russian president, and the warning

in this regard came from Oslo to the General Staff 3 weeks earlier. This was also confirmed by the Chief of the General Staff, Mikhail Kolesnikov[17].

Accordingly, the threat of nuclear war can arise for various reasons. However, the most important thing is that the issue of nuclear security should not be entrusted to artificial intelligence and computer systems, because the human factor is very important in security policy, because it has the ability to make rational and correct judgments in crisis situations.

Conclusion

The synthesis of AI and weapons of mass destruction presents humanity with both a set of opportunities and many threats. As artificial intelligence continues to develop every day, which also enhances the capabilities of weapons of mass destruction, this is a matter of concern. These systems also enable innovative solutions that are also helpful in detecting, preventing and mitigating these threats.

Ethical norms of artificial intelligence technologies in the direction of weapons of mass destruction require effective verification and strict control. International cooperation, transparent policies and strong regulatory frameworks are essential to ensure that artificial intelligence systems are used responsibly for good rather than threats.

The findings indicate that power grid analysis, picture analysis to detect concealed and protected places, and communications metadata analysis to identify key players and their involvement in proliferation networks are the most potential machine learning applications in Counter-WMD. Artificial intelligence in the far future might be able to predict nuclear decision points, monitor proliferator progress, and create new frameworks for arms reduction.

More coordination and collaboration between various businesses and nations to create shared protections for AI development is probably going to ease geopolitical tensions and deter relevant entities from promoting the military use of their AI technologies. Examining how old and new dangers merge will become essential to maintaining and enhancing national and international security as all of these technologies grow at an accelerated rate and nuclear tensions reach an almost unprecedented level. There are worries about increased dangers of accidental or deliberate use of nuclear weapons, decreased crises stability, and new arms races at the nexus of AI and nuclear weapons.

[17] *Who is the man who saved the world from a nuclear disaster*, Tbilisi 2021, p. 1, <https://intermedia.ge> (12.11.2024).

BIBLIOGRAPHY:

1. Boulanin V., *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, Stockholm International Peace Research Institute 2019, Vol. I Euro-Atlantic Perspectives, <https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf>
2. Caruso C., *The Risks of Artificial Intelligence in Weapons Design*, Harvard College 2024, <https://hms.harvard.edu/news/risks-artificial-intelligence-weapons-design>
3. Caves J. P., Carus W. S., *The Future of Weapons of Mass Destruction: Their Nature and Role in 2030*, National Defense University Press, Washington 2014, <ndupress.ndu.edu/Portals/68/Documents/occasional/cswmd/CSWMD_OccationalPaper10.pdf>
4. Chernavskikh V., *Nuclear weapons and artificial intelligence: technological promises and practical realities*, 2024, <https://www.sipri.org/sites/default/files/2024-09/bp_2409_ai-nuclear.pdf>
5. Cleobury S., *Artificial Intelligence and Arms Control – How and Where to Have the Discussion*, Geneva Centre for Security Policy 2023, <https://www.gcsp.ch/publications/artificial-intelligence-and-arms-control-how-and-where-have-discussion>
6. Donaldson R., *Sounding the alarm on AI-enhanced bioweapons*, European Leadership Network 2024, <https://europeanleadershipnetwork.org/commentary/sounding-the-alarm-on-ai-enhanced-bioweapons/>
7. Dresp-Langley B., *The weaponization of artificial intelligence: What the public needs to be aware of*, National Library of Medicine, <https://pmc.ncbi.nlm.nih.gov/articles/PMC10030838/>
8. *Four cases when the world was on the verge of nuclear war*, Tbilisi 2019, <https://geostate.ge>
9. Guersenzvaig A., *Autonomous Weapon Systems: Failing the Principle of Discrimination*, "IEEE Technology and Society Magazine" 2018, Vol. 37, Issue: 1, 2018, <https://ieeexplore.ieee.org/abstract/document/8307136/authors#authors>
10. James J., Eleanor K., *AI, Cyberspace, and Nuclear Weapons*, "War on the Rocks" 2020, <https://warontherocks.com/2020/01/ai-cyberspace-and-nuclearweapons/>
11. Kim A., *Regulating Further Scientific Development of Mass Destruction Weapons with Regards to Artificial Intelligence*, Disarmament Commission MUNiSC 2021,

<https://mun.isqchina.com/wpcontent/uploads/2021/01/DA_04_Regulating-Further-Scientific-Development-of-Mass-Destruction-Weapons-with-Regards-to-Artificial-Intelligence.pdf>
12. Kukuruznyak D., *Can Artificial Intelligence be a Weapon of Mass Destruction?*, Max Planck Institute for Solid State Research 2023, <https://hal.science/hal-04101741>
13. Meier O., *The fast and the deadly: When Artificial Intelligence meets Weapons of Mass Destruction*, 2024, <https://european-leadershipnetwork.org/commentary/the-fast-and-the-deadly-when-artificial-intelligence-meets-weapons-of-mass-destruction/>
14. *Proceed with Caution: Artificial Intelligence in Weapon Systems, AI in Weapon Systems Committee*, Report of Session 2023-2024, published by the Authority of the House of Lords, <https://publications.parliament.uk/pa/ld5804/ldselect/ldaiwe/16/16.pdf>
15. Puwal P. S., *Should artificial intelligence be banned from nuclear weapons systems?*, NATO 2024, <https://www.nato.int/docu/review/articles/2024/04/12/should-artificial-intelligence-be-banned-from-nuclear-weapons-systems/index.html>
16. Shakirov O., *Russian Thinking on AI Integration and Interaction with Nuclear Command and Con trol, Force Structure, and Decisionmaking*, European Leadership Network, London 2023
17. *What are the rules for launching nuclear weapons?*, Tbilisi 2022, <https://www.radiotavisupleba.ge/a/31735977.html>
18. *Who is the man who saved the world from a nuclear disaster*, Tbilisi 2021, <https://intermedia.ge>

„Ante Portas – Security Studies”
2024, No. 21
DOI: 10.33674/1202420

Svetlana CEBOTARI[1]
Moldova
Victoria BEVZIUC[2]
Moldova

THE COMMON SECURITY AND DEFENSE POLICY OF THE EUROPEAN UNION IN THE CONTEXT OF THE WAR IN UKRAINE

Abstract: *The emergence of the war in Ukraine, conditioned by the occupation of the Crimean Peninsula in 2014 and the invasion of the Russian Federation in 2022 is, since the collapse of the Soviet Union, the event that will have the greatest geopolitical implications for the international arena, including the European Union, in particular the Common Security and Defense Policy. The ongoing war involves a number of long-term effects on the security and stability of the European continent. The degree of possibility of some of the consequences of the Russian-Ukrainian war will be negligible and will be the subject of debates for academia, but also for Western political leaders for many years to come. The purpose of this article is to highlight the main issues that have taken place in the Common Security and Defense Policy of the European Union as a result of the outbreak of war in Ukraine. This will analyze the steps taken by the EU to ensure peace on the European continent. Some aspects of EU-NATO cooperation in the context of the war in Ukraine will also be highlighted.*

Keywords: *aggression, conflict, war, Ukraine, politics, security, European Union*

Introduction

The main feature of the 21st century is the presence of Russian-Western rivalry manifested mainly by the Russian-Ukrainian War, a war conditioned by

[1] Svetlana Cebotari, PhD, DSc, Moldova State University (Moldova), ORCID: 0000-0001-9073-104X, email: svetlana.cebotari11@gmail.com
[2] Victoria Bevziuc, PhD, Moldova State University (Moldova), ORCID: 0000-0001-9189-641X, email: victoriabevziuc@yahoo.ro

the unjustified invasion of the Russian Federation in Ukraine. The war in Ukraine marks the geopolitical rivalry in relations between Russia, the European Union (EU) and the United States (USA). It is also an unprecedented break in the Euro-Atlantic security order, which has deteriorated considerably since 2008[3]. The result of the war in Ukraine is, since the collapse of the Soviet Union, the event that will have the greatest geopolitical implications on the international arena, including the European Union. The degree of possibility of some of the consequences of the Russian-Ukrainian war will be negligible and will be the subject of debates for academia, but also for Western political leaders for many years to come[4].

Russia's invasion of Ukraine and the ongoing war involve a number of long-term effects on the security and stability of the European continent. The civil wars in Yugoslavia in the 1990s, the terrorist attacks on cities in the European space in the years 2000 and 2010, the destabilization of North Africa and the Middle East in 2011 and the occupation of Crimea by 2014, and, more recently the unjustified invasion of Ukraine by the Russian Federation has led the European Union to adopt a common security and defense policy[5].

Thus, in order to highlight the main aspects of the impact of the war in Ukraine on the Common Security and Defense Policy of the European Union, as well as for the purpose of elaborating this research we used a set of general-specific research methods, such as: phenomenological method, historical method and web graphic method.

The phenomenological method, as a method of research in philosophy, allowed the examination of the fundamental conditions and events („ phenomena" which contributed to the acceleration, or the strengthening of the Common Security and Defense Policy of the European Union in the context of the war in Ukraine conditioned by the occupation of the Crimean Peninsula in 2014 and the unjustified invasion of 2022 by the Russian Federation.

The use of the historical method allowed analyzes to be carried out on the strengthening of the EU Security and Defense Policy in the context of the war in Ukraine. There is still no research in the scientific literature of the Republic of Moldova on the impact of the war in Ukraine on the strengthening of EU security policy, the use of the web graphic method was used, which offered the

[3] F. Steinberg, J. Tamames, *La UE en el mundo tras la guerra de Ucrania*, <https://www.realinstitutoelcano.org/analisis/la-ue-en-el-mundo-tras-la-guerra-de-ucrania/> (12.02.2024).

[4] *Invasión rusa a Ucrania cambiara el entorno de seguridad de Europa "durante décadas"*, <https://www.vozdeamerica.com/a/invasion-rusa-de-ucrania-cambio-el-entorno-de-seguridad-de-europa-durante-decadas-/6977069.html> (12.02.2024).

[5] A. Marrone, *Dove va la sicurezza europea?*, <https://www.affarinternazionali.it/la-guerra-russo-ucraina-e-le-sfide-per-la-sicurezza-europea/> (12.02.2024).

possibility to examine the issue submitted to the research at theoretical and practical level from the main sources published on the websites.

European security and defense policy in the context of the war in Ukraine

Over the last three decades, that is, since the end of the Cold War, security and defense issues have held a relatively peripheral position for the European political class. Presence of an active war for more than a year, high intensity on the European continent has led to an exponential increase in political and information interest in security and defense issues. Although since 1999, more than 23 years, the EU has a Common Security and Defense Policy (CSDP) - in reality (CSDP), former European Security and Defense Policy or ESDP) was not really well outlined. Since 1999, European leaders have made it clear that the CSDP's goal was to provide Europe with the capabilities and mechanisms needed to conduct crisis management operations abroad, i.e. peacekeeping and stability operations in conflict zones. The territorial defense and deterrence against potential threats from European states were primarily within the competence of the North Atlantic Treaty Organization (NATO). Thus, over the years, EU defense policy has therefore been a security policy, which has prioritized low- and medium-intensity capabilities and operations, as evidenced by experiences in the Balkans, Africa, the Middle East and Afghanistan.

The EU's emphasis on crisis management operations abroad can be explained by the fact that territorial defense and deterrence were NATO's objectives, which has an integrated and consolidated command structure, and the strategic and political opinion is represented by the leadership of the United States of America (USA). On the other hand, in the late 1990s, with the launch of the CSDP, defense and deterrence seemed to become superfluous, given the geopolitical and technological-military hegemony of the USA and the West. In this context, NATO itself is launching in the field of managing operations abroad, such as those in the Balkans and Afghanistan. Thus, in the last two decades, we see NATO and the EU coexisting in the field of crisis management operations abroad, with NATO generally dealing with, of those tasks which may involve fighting (high and medium-high intensity) and EU- involved in stabilization tasks bordering the police sphere and finding added value in the connection between the military (low intensity) and „ civil" (police tasks, judicial advice or administrative and development policies). This task-sharing logic has worked over the last two decades, from the launch of the CSDP in 1999 to the last years. Now, however, we are entering a radically different geostrategic context, in which issues related to territorial defense and the discouragement of the great powers are again regaining their primacy in the debates on security policy. The return of threats from states such as the Russian Federation indicates a greater interest in defense, but also a different way of

approaching defense issues, by focusing on territorial defense and deterrence to the detriment of crisis management operations abroad[6].

The shock has also served in the international system in recent years as alarm signals for the European Union to be aware of the need to strengthen its defense capabilities. First, in the summer of 2021, the withdrawal of the US and NATO from Afghanistan, perceived as a substantial failure by the entire Western world has led many European leaders to return to the concept of „strategic autonomy". About six months later, the Russian invasion of Ukraine again forced European leaders into a new geopolitical reality[7].

What is European defense specifically? The concept is in fact more evasive and less concrete. CSDP is, in essence, the political framework through which European Member States can develop a strategic culture with reference to security and defense, can jointly address conflicts and crises, they can protect the Union and its citizens and strengthen international peace and security. Over the years the EU has been endowed with specific financial, financial and cooperation instruments in the field of public or other procurement. The idea of the Common Security and Defense Policy dates back to 1948, when France, the United Kingdom and the Benelux countries signed the Brussels Treaty, which in 1954 led to, when the Western European Union was established, a political-military alliance that remained virtually inactive until the' 90s. The idea of creating a European army also dates back to the 1950s, although it has never been implemented before: France, in fact, after proposing the creation of the European Defense Community (CEDE), it did not ratify the Treaty. Since the 1990s, the themes of defense and security have once again taken up space in the European debate, with a number of initiatives leading precisely to the establishment of a common foreign and security policy framework and the strengthening of cooperation with NATO, making it more structured and sustainable. Moreover, concrete steps are being taken in the next three decades to seek the creation of a common strategic culture, as well as in launching initiatives to better integrate the armed forces of the Member States. The European Defense Agency (EDA) was established in 2004, the European External Action Service (EEAS or EEAS) was established in 2009, and a first relevant strategic document, the comprehensive European strategy was published in 2016. In addition, PESCO (Permanent Structured Cooperation) was launched in 2017, allowing Member States wishing and able to develop

[6] L. Simón, *Autonomía estratégica y defensa europea después de Ucrania*, <https://www.realinstitutoelcano.org/analisis/autonomia-estrategica-y-defensa-europea-despues-de-ucrania/> (12.02.2024).
[7] *Ibidem*.

defense capabilities together, investing in joint projects for the benefit of their armed forces and, consequently, of operational capacity at European level[8].

Just one month after the Russian Federation's invasion of Ukraine, the Ministers of Foreign Affairs and Defense of the member countries of the European Union adopted on March 10, 2023, in Brussels, at a time when we are witnessing the return of war to Europe, European Defense Strategic Compass – a new common defense policy that will allow the EU to establish rapid reaction forces[9]. The aim of the strategic compass is to make the EU a stronger and more capable security provider. The EU must be able to protect its citizens and contribute to international peace and security. This is all the more important at a time when the war returned to Europe, following Russia's unjustified and unprovoked aggression against Ukraine, and also at a time of major geopolitical transformations. This Strategic Compass will strengthen the EU's strategic autonomy and its ability to work with partners to protect its values and interests[10].

A stronger and more capable EU in terms of security and defense will make a positive contribution to global and transatlantic security and complement NATO, which remains the basis of collective defense for its members. The EU will also step up its support for the rules-based world order, at the heart of which the United Nations is at the heart. The threats are rising and the cost of inaction is clear. The strategic compass is a guide to action. It sets out an ambitious path for our security and defense policy for the next decade. It will help us take responsibility for security, in front of our citizens and the rest of the world. The strategic compass provides a joint assessment of the strategic environment in which the EU carries out its actions and of the threats and challenges facing the Union. The document presents concrete and achievable proposals, with a very precise implementation timetable, to improve the EU's capacity to act decisively in crisis situations and to defend its security and its citizens. The compass covers all aspects of security and defense policy and is structured around four pillars: action, investment, partnerships and security[11]. The publication of the Strategic Compass, which set concrete goals to be

[8] A. Marrone, *Dove va la sicurezza europea?*, https://www.affarinternazionali.it/la-guerra-russo-ucraina-e-le-sfide-per-la-sicurezza-europea/> (12.02.2024).

[9] *Une boussole stratégique pour l'UE*, <https://www.consilium.europa.eu/fr/infographics/strategic-compass/> (12.02.2024).

[10] *Une boussole stratégique pour renforcer la sécurité et la défense de l'UE au cours de la prochaine décennie*, <https://www.consilium.europa.eu/fr/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/> (12.02.2024).

[11] *Ibidem*.

achieved by 2025, is a more decisive and concrete document as opposed to the 2016 Global Strategy[12].

Thus, the "Action" pillar provides that in order to be able to act quickly and firmly whenever a crisis breaks out, with partners if possible and on their own when necessary, the EU:

- will establish a strong EU rapid deployment capacity of up to 5,000 troops for various types of crises;
- will be prepared to conduct a CSDP mission of 200 fully equipped experts within 30 days, including in complex environments;
- will perform regular real exercises on land and at sea;
- will increase military mobility;
- will strengthen CSDP missions and operations (common security and defense policy) civilian and military promoting faster and more flexible decision-making, acting more firmly and ensuring greater financial solidarity;
- will make full use of the European Peace Instrument to support partners.

For the second pillar "Security", the EU will strengthen its capacity to anticipate, to discourage and respond to current and emerging rapidly evolving threats and challenges, as well as to protect the EU's security interests. To this end, the EU:

- will strengthen its information analysis capabilities;
- will develop a set of tools to counter hybrid threats and response teams in the event of hybrid threats that bring together various tools whose role will be to detect a range wide hybrid threats and respond to them;
- will further develop the toolkit for cyber diplomacy and establish an EU cyber defense policy to increase preparedness and respond to cyber-attacks;
- will develop a set of tools for foreign information manipulation actions and for foreign interference;
- will develop an EU space strategy for security and defense;
- will strengthen the EU's role as an actor in the field of maritime security.

The third pillar of the Strategic Compass "Investments" requires the Member States to substantially increase their defense spending in order to respond to the collective ambition to reduce critical deficiencies in military and

[12] C. M. Banu, *Politica de securitate și apărare comună a UE – de la Strategia globală (2016) la Busola strategică (2022). Spre reconfigurare prin efectul războiului din Ucraina? Studiu* (12.02.2024).

civilian capabilities and to strengthen the European defense industrial and technological base. In this context, the EU:

- will exchange national targets for increasing and improving defense spending to meet our security needs;
- will provide additional incentives for the Member States to engage in collaborative capacity building and to invest jointly in strategic support factors and new capabilities generation of operating on land, sea, air, cyberspace and outer space;
- will drive technological innovation in the field of defense to close strategic gaps and reduce technological and industrial dependencies.

For the fourth pillar "Partnerships", in order to address common threats and challenges, the EU:

- will strengthen cooperation with strategic partners such as NATO, the UN and regional partners, including the OSCE, the AU and ASEAN;
- will develop more appropriate bilateral partnerships with countries and strategic partners who share the same vision, such as the USA, Canada, Norway, the United Kingdom, Japan and others;
- will develop adapted partnerships in the Western Balkans, in our eastern and southern neighborhood, in Africa, Asia and Latin America, including by increasing dialogue and cooperation, promoting participation in CSDP missions and operations and supporting capacity building[13].

Thus, the EU Strategic Compass will help to strengthen a common European culture of security and defense and to define the right objectives and concrete goals for EU policies. It will address four different, interconnected areas: – crisis management missions; resilience; tools and capabilities; cooperation with partners. From this perspective, the EU Strategic Compass resembles the NATO programmatic document – The Strategic Concept – which sets out three pillars: collective defense, crisis management and security through cooperation. In fact, the adoption of the EU Strategic Compass was followed by the adoption of the next NATO Strategic Concept at the Madrid Summit on 29-30 June 2022[14].

Collaboration with NATO has also been strengthened by the signing of a new cooperation agreement - Joint Declaration signed on 10 January 2023. This is the third joint statement, following the Warsaw Declaration of 2016 and the

[13] A. Marrone, *Dove va la sicurezza europea?*, <https://www.affarinternazionali.it/la-guerra-russo-ucraina-e-le-sfide-per-la-sicurezza-europea/> (12.02.2024).

[14] R. Lupițu, *UE aprobă luni Busola strategică a apărării, care prevede o forță militară de 5.000 de soldați și creșterea cheltuielilor pentru apărare*, <https://www.caleaeuropeana.ro/ue-aproba-luni-busola-strategica-a-apararii-care-prevede-o-forta-militara-de-5-000-de-soldati-si-cresterea-cheltuielilor-pentru-aparare/> (12.02.2024).

Brussels Declaration of 2018, as part of a partnership of over twenty years. The most significant aspect is probably the declaration of desire for „ further strengthening of cooperation (EU and NATO) in existing areas, as well as its extension and deepening, in particular as regards geostrategic competition, resilience issues, critical infrastructure protection, and disruptive technologies, space, climate change security implications, as well as the manipulation of information and the interference of foreign actors.

In this sense, the most interesting innovation brought by the Strategic Compass was the proposal to create, by 2025, a rapid reaction capacity (European Rapid Deployment Capacity (EU DRC), in order to allow troops to deploy up to a maximum of 5,000 units in a non-permissive environment in response to different types of crises. About one year after the publication of the Strategic Compass on March 9, 2023, The European Parliament's Foreign Affairs Committee (AFET) approved a report to better define the characteristics to be assigned to this new instrument, which is considered key to the strategic autonomy of the European Union. The draft was then presented in plenary, which approved the resolution entitled EU Rapid Deployment Capacity (CDR), EU Battle Groups and Article 44 of the EU Treaty (TUE): "The path to follow".

The comparison between the EU's Rapid Deployment Capacity and EU fighting groups has been inevitable since the presentation of this new instrument, although in a closer analysis the two instruments differ substantially significantly. EU combat groups are defined as „ multinational military units, generally composed of 1,500 staff each and are an integral part of the European Union's rapid response military capability to respond to emerging conflicts and crises around the world". These combat groups have been operational since 2007 and have contributed as a tool for defense cooperation and transformation, but for various reasons they have never been carried out at operational level. As an instrument falling under the CSDP umbrella, in fact, the decision on their use must be approved unanimously by all Member States. In addition – can be an even more decisive factor in discouraging their use – their operation provides for troops to be supplied on a rotating basis by Union countries and as their possible use be fully funded by any state that contributes in terms of people and equipment. For the CDR, the EU has decided to provide funding at central level. However, as these are measures relating to the Common Security and Defense Policy, the decision-making power remains in the hands of the Member States[15].

[15] S. Samorè, *Il momento della difesa europea: prospettive e criticità a più di un anno dall'invasione dell'Ucraina*, <https://www.pandorarivista.it/articoli/il-momento-della-difesa-europea-prospettive-e-criticita-a-piu-di-un-anno-dall-invasione-dell-ucraina/> (12.02.2024).

Russia's invasion of Ukraine a year ago triggered a long-term transformation in European defense policy. The war in Ukraine has produced unprecedented political convergence in Europe, with a unanimous perception of the need to increase defense capacity. This unanimity corresponds to a renaissance of NATO's collective security dimension. But we can still ask ourselves the question of the future of this consensus on the use of a European Union military force. Suppose that the Council of the European Union already has the power to mobilize a rapid action force of 5,000 people, as proposed in the Strategic Compass. In the current context, it could certainly have helped to strengthen the Union's defense position in the neighboring Member States with Ukraine or Russia. Exactly what some EU and NATO members have already done in the NATO Response Force (NRF), whose capabilities have already been increased since 2014. If we expand the current scenario, it would seem difficult to think of a possibility of EU military intervention that does not fall within NATO's policy in Europe. A direct intervention of an EU force in Ukraine while NATO would remain defensively would be a misinterpretation at various levels. It would then be necessary to consider using this force in other scenarios „ outside NATO" (evacuation of citizens, peacekeeping interventions for low-intensity commitments, etc.)[16]

The current political moment is favorable to defense. It makes it possible to put the military issue back at the heart of the European debate, a return to a principle of desirable realism after a period marked by a paradigm of European economic and normative growth. Leaving aside the operational aspect of European forces that remain directly controlled by the Member States, it is also, legitimately, we think that the various statements of increases in military budgets could allow a real leap in the European military industry. The prospect of an integrated and unified civilian and military technology market at European Union level with the strengthening of strong public demand would allow for extremely favorable conditions for development, taking into account an existing mechanism in the United States, where defense spending plays an important role in technology development. Moreover, there are already institutional mechanisms, such as the European Defense Agency (AED), which are able to carry out joint military technological development programs and which can certainly benefit greatly from an increase in budgets.

The war in Ukraine is also a key moment in developing a European strategic autonomy. This political statement, which has been a real success since last year, offers the opportunity to benefit from the progress of the programs already launched by the commission by adding military spending to the

[16] *Invasión rusa a Ucrania cambiara el entorno de seguridad de Europa "durante décadas"*, <https://www.vozdeamerica.com/a/invasion-rusa-de-ucrania-cambio-el-entorno-de-seguridad-de-europa-durante-decadas-/6977069.html> (12.02.2024)

common benefit. From this point of view, the Strategic Compass seems very weak because, if it evokes, through various measures, a strengthening of cooperation with a mechanism to stimulate multilateral cooperation in defense. Therefore, it would be desirable to rapidly amplify it with a European plan on the military side of „technological sovereignty" to prevent the restoration of autarchic reflexes in terms of defense spending and chapel multiplication which annihilates the effects of critical mass and technological progress.

Based on these reasoning, the conditions for a future vision of European defense should be laid down. The project to create European rapid response forces bringing together the contributions of different Member States, in order to have a common instrument that makes it possible for Europe to collective defense, which would in itself be a form of political response to the presence of war on the European continent[17].

The war in Ukraine has changed not only relations between Russia and the rest of Europe, but also relations between the Member States of the European Union (EU) and the North Atlantic Treaty Organization (NATO). Currently, in the context of the war in Ukraine, a new balance is emerging between the states belonging to Western Europe, on the one hand, and the states of Central and Eastern Europe, Baltic states (Estonia, Latvia, Lithuania) and northern European states (Norway, Denmark, Finland and Sweden). Prior to the war in Ukraine, the states of Northern Europe and Central and Eastern Europe were considered, in all respects, as a „ junior partner" within the EU, given the supremacy of Franco-German relations that shaped and guided the debates on collective security issues. Under French influence, Western Europe has worked with both the EU and NATO to create a strategic military autonomy for Europe. The war in Ukraine has made this strategic orientation absolute.

The Eastern part of the North Atlantic Alliance consists of three groups of states, stretching from the Baltic Sea in the North to the Black Sea in the South, it is now forming the Eastern flank of NATO, which considers the United States to be the most important ally for protecting security, as well as for defending liberal democracies in Europe. The Eastern part of NATO perceives the United States as a key ally, able to balance the relationship between NATO's two wings (East and West). Neither France nor Germany, for various reasons, are able to do so. In fact, the United States resumed, under the presidency of Joe Biden, the same role they played in the most acute phase of the Cold War (1947-1962). The United States' commitment to Ukraine and its desire to ensure the security of Eastern NATO have set aside the false assumption that it is moving away from Europe, pivoting towards Asia, to

[17] *La relance de la défense européenne et le conflit en Ukraine : dynamiques et paradoxes*, <https://www.frstrategie.org/publications/notes/relance-defense-europeenne-conflit-ukraine-dynamiques-paradoxes-2022> (12.02.2024).

control China, which tends to annex Taiwan by force. President Xi Jinping's visit to Moscow on March 20-22, 2023, sealed the alliance, already forming for several years, between China and Russia. This new geopolitical reality presupposes the military presence of the United States in Central and Eastern Europe, essential for both European and Asian security. Following Russian aggression against Ukraine, NATO states have seen that without the decisive contribution of the United States, the war could have ended in 2022 with the defeat of Ukraine and the deletion of its state in favor of Russia. The strategic axis linking NATO's eastern flank and the United States thus emerged following Russian aggression on February 24, 2022, and was implemented during President Biden's visit to Kiev and Warsaw on February, 21 and 22, 2023.

In the Poland capital, the US president met with the nine heads of states from the Central and Eastern Europe, thanking them for their support for Ukraine since the beginning of Russian aggression. Following this meeting, the states of northern Europe (Norway, Denmark, Finland and Sweden) decided to further integrate their air forces, by signing NATO in Germany, a statement to that effect. These countries have more than 300 fighter jets, a considerable force that contributes to discouraging and defending NATO. This military cooperation allows Sweden (pending its accession to NATO, currently blocked by Turkey) to prepare its armed forces for integration into the Alliance system.

Of the Central and Eastern European states, two states – Poland and Romania – are at the forefront of NATO defense. Both states have a long border with Ukraine and have accepted hundreds of thousands of Ukrainian refugees on their territory. One year after the outbreak of war in Ukraine, Poland significantly increased its armed forces. Its military budget for 2022 is 2.4% of GDP. The goal for 2023 is to reach 4%, well above the 2% and desired by the 30 NATO members. The Polish army has 170,000 soldiers, a size comparable to that of Germany. Poland intends, according to Defense Minister Mariusz Blaszczak, to increase its army number to 300,000 troops in the coming years, to become the largest army in Europe. In turn, Romania has an army of 70,000 active soldiers, 60,000 members of the paramilitary forces and 55,000 reservists. Since the beginning of the war in Ukraine, the country has doubled its investment in the military industry, allocating significant amounts in the purchase of military equipment. During 2023, Romania will host a defense innovation accelerator for research into new technologies that currently concern the military sectors: artificial intelligence, biotechnologies and innovative materials. Also, a major missile shield was installed in Romania at

Deveselu. Also, at the Mihail Kogălniceanu military base, located 185 kilometers east of Bucharest, 2,000 American soldiers[18] are stationed.

Conclusions

Currently, the European security architecture is going through a redefining phase, being determined by crises and multidimensional challenges, especially being redefined by the emergence of war in Ukraine. The invasion of Ukraine by the Russian Federation has marked a turning point for Europe and will mark the memory of future generations. On the other hand, the Russian invasion made the European Union more united and that all its members — including Poland and Hungary to align themselves against the actions of the Russian Federation in Ukraine. We have also been present at the reactions of historically neutral countries, such as Sweden and Finland, which have reiterated their right to join NATO, and Switzerland, which has adhered to the economic sanctions of the European Union.

We are currently present at strengthening the military capabilities and capabilities of the European Union, the purpose of which is to ensure security on the European continent. Also, in the context of the war in Ukraine, we are present not only to promote Europe's strategic autonomy, but also to strengthen EU-NATO cooperation in ensuring European security, which in the future, will cause Russia to face a militarily strengthened Europe.

BIBLIOGRAPHY:

1. Banu C. M**.,** *Politica de securitate și apărare comună a UE – de la Strategia globală (2016) la Busola strategică (2022). Spre reconfigurare prin efectul războiului din Ucraina? Studiu*
2. *Invasión rusa a Ucrania cambiara el entorno de seguridad de Europa "durante décadas"*, <https://www.vozdeamerica.com/a/invasion-rusa-de-ucrania-cambio-el-entorno-de-seguridad-de-europa-durante-decadas-/6977069.html>
3. *La relance de la défense européenne et le conflit en Ukraine : dynamiques et paradoxes*, <https://www.frstrategie.org/publications/notes/relance-defense-europeenne-conflit-ukraine-dynamiques-paradoxes-2022>

[18] *La sicurezza Europea di fronte a crisi multidimensionali prospettive future e collocazione dell'italia*, <https://www.esteri.it/wp-content/uploads/2023/05/Paper-sicurezza-Maeci-IAI-DEF.pdf> (12.02.2024).

4. *La sicurezza Europea di fronte a crisi multidimensionali prospettive future e collocazione dell'italia*, <https://www.esteri.it/wp-content/uploads/2023/05/Paper-sicurezza-Maeci-IAI-DEF.pdf>
5. Lupiţu R., *UE aprobă luni Busola strategică a apărării, care prevede o forță militară de 5.000 de soldați și creșterea cheltuielilor pentru apărare*, <https://www.caleaeuropeana.ro/ue-aproba-luni-busola-strategica-a-apararii-care-prevede-o-forta-militara-de-5-000-de-soldati-si-cresterea-cheltuielilor-pentru-aparare/>
6. Marrone A., *Dove va la sicurezza europea?*, <https://www.affarinternazionali.it/la-guerra-russo-ucraina-e-le-sfide-per-la-sicurezza-europea/>
7. Samore S., *Il momento della difesa europea: prospettive e criticità a più di un anno dall'invasione dell'Ucraina*, <https://www.pandorarivista.it/articoli/il-momento-della-difesa-europea-prospettive-e-criticita-a-piu-di-un-anno-dall-invasione-dell-ucraina/>
8. Simón L., *Autonomía estratégica y defensa europea después de Ucrania*, <https://www.realinstitutoelcano.org/analisis/autonomia-estrategica-y-defensa-europea-despues-de-ucrania/>
9. Steinberg F., Tamames J., *La UE en el mundo tras la guerra de Ucrania*, <https://www.realinstitutoelcano.org/analisis/la-ue-en-el-mundo-tras-la-guerra-de-ucrania/>
10. *Une boussole stratégique pour l'UE*, <https://www.consilium.europa.eu/fr/infographics/strategic-compass/>
11. *Une boussole stratégique pour renforcer la sécurité et la défense de l'UE au cours de la prochaine décennie*, <https://www.consilium.europa.eu/fr/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/>

„Ante Portas – Security Studies”
2024, No. 21
DOI: 10.33674/1202421

Krzysztof SURDYK[1]
Poland

THE IMPACT OF THE ECONOMIC AND FINANCIAL WAR WITH RUSSIA ON THE FUNCTIONING OF THE WESTERN ECONOMY

Abstract: *In the current confrontation between Russia and the broadly understood West, we are not only dealing with military struggles. It can be said that military operations in Ukraine are just one element of the global confrontation. Economic and financial operations are at the forefront, which are intended to inflict losses on the opponent, forcing them to make concessions or even capitulate. The aim of the article was to draw attention to the threats that Western countries may face, directly or indirectly involved in conducting economic activities. It indicates what threats may appear in the economic and financial spheres. It turns out that some of these threats may result from deliberate counteraction by the opponent (in this case the Russian Federation), and some may arise in connection with the indefiniteness of economic wars, with phenomena in politics, economy, finance, etc. that are difficult to predict. Sometimes we are not fully able to predict what consequences prohibitive tariffs and sanctions that were to hit our opponent will have for us.*

Keywords: *economic war, sanctions, energy resources, industry, production costs, financial system*

Introduction

Economic and financial wars are an essential component of every hybrid war. The range of actions of states deciding to conduct economic and financial wars is very diverse, depending on the economic potential and financial capabilities of a given state. When preparing hybrid operations in the economic sphere, it is important to predict all possible effects of the actions taken. One of

[1] Krzysztof Surdyk, PhD, Helena Chodkowska University of Technology and Economics (Poland), ORCID: 0009-0002-0654-4095, e-mail: krzysztof.surdyk@interia.pl

the tools necessary to carry out an attack on the economy of the attacked country is to prepare a "strike plan", taking into account the economic situation of the target country, its specific situation in the spheres of production, distribution, exchange and consumption. In such a plan, it is also important to determine the level of development of the opposing state in each of the above-mentioned areas, as well as to determine the thresholds, exceeding which may have a significant impact on the functioning of both these spheres and the economy as a whole[2]. On the other hand, the "economically attacked" state should retain the ability to reveal the nature of the emerging danger in order to effectively counter the model of chaos in the economic sphere used against it. Neutralization of external and internal economic threats requires the introduction of significant adjustments in the state's macroeconomic policy. Development of specific industrial sectors of the economy, development of the military-industrial complex and balanced financial policy. Predicting possible actions of the aggressor country and the effects of processes initiated using the economic warfare model is of paramount importance for defense against a possible attack and weakening or complete destruction of the economy. Economic and financial wars against economically weaker opponents do not require such complicated procedures. In many cases, economic sanctions, blocking the accounts of individual politicians, enterprises, and sometimes economic blockade of the opposing country are sufficient. Of course, various types of sanctions are more effective when we include our allies in them, and also deprive the opponent of the possibility of economic maneuver and sources of financing. We can see such solutions in the actions of the United States towards Russia, which has included most of its allies in this war. Russia is trying to respond, but its economic countermeasures are limited. This does not mean that we can ignore the threats that may affect the West, on the occasion of such actions.

Russia's Economic Game with the West

Russia's military invasion of Ukraine has provoked a hybrid reaction from the West. A number of diplomatic, informational, technological, and primarily economic and financial actions have been taken against Moscow, the aim of which is to limit the country's ability to conduct combat operations against Ukraine. Tens of thousands of economic sanctions, export and import restrictions have been introduced on Russian companies, enterprises, banks, and research institutes, including primarily the Russian fuel and energy sector.

[2] K. Surdyk, *Konflikt ukraiński w rozgrywkach geopolitycznych*, Warszawa 2017, pp. 115-118.

Economic threats to the West

Although Russia is suffering huge losses from the ongoing economic war, it also unfortunately carries the risk of serious macroeconomic consequences for the West. These include: slowing economic growth, even higher inflation and possibly even stagflation, rising unemployment and falling consumer confidence, etc. The prolonged conflict is likely to lead to downward revisions to sales forecasts. The effects of the ongoing war against Ukraine and its geopolitical repercussions – continued sanctions, trade bans with Russia, supply disruptions, higher military spending – mean that the crisis in Ukraine could have as big or even a longer-term impact on the global and European economy as the COVID-19 crisis and its aftermath[3]. "The world economy was already struggling with numerous challenges before the war (in Ukraine - author's note), such as lockdowns during the pandemic, climate change, energy problems. The migration crisis was smoldering. Now, as a result of Russia's aggression against Ukraine, there are problems with millions of refugees from Ukraine, problems with food, including grain supplies, energy crisis and high inflation"[4]. In addition, the war in Ukraine also brought a food and energy crisis, which are also inflationary factors.

First, energy. Energy prices have been volatile since mid-2021. In the Versailles Declaration of March 2022, the leaders of the 27 EU member states agreed to end the EU's dependence on Russian fossil fuel imports as soon as possible. On 30-31 May 2022, the European Council decided that by the end of 2022, the EU would stop importing almost 90% of its oil from Russia, with a temporary derogation only for oil delivered via pipelines[5]. Russia previously supplied Europe with around 140 billion cubic meters of pipeline gas, but in 2022 it supplied only 76 billion cubic meters, half as much. Europe has managed to cope with this problem, albeit with heavy losses. In 2023, Russia supplied around 25 billion cubic meters of gas, including gas transported via the Turkish Stream and transit through Ukraine. Of course, even in such conditions, Europe is coping; no one freezes in winter. However, Europe is paying high bills for becoming independent from Russian gas. These include,

[3] W. Kukuła, *Skutki wojny na Ukrainie – długoterminowe ryzyka dla globalnej motoryzacji*, <https://magazyn.cartrack.pl/wojna-na-ukrainie-konsekwencje-dla-motoryzacji/> (20.10.2022).

[4] V. Movchan, Research Director at the Institute of Economic Analysis and Policy Consulting in Kijev, statement during the debate on „Krynica Forum '22 – Wzrost i Odbudowa", <https://www.rp.pl/wydarzenia-gospodarcze/artykul/37296281-wplyw-wojny-w-ukrainie-na-gospodarke> (25.10.2022).

[5] *Rynkowe skutki rosyjskiej inwazji na Ukrainę: reakcja UE*, <https://www.consilium.europa.eu/pl/policies/eu-response-ukraine-invasion/impact-of-russia-s-invasion-of-ukraine-on-the-markets-eu-response/> (25.10.2022).

among others: a one-third drop in income in industry, billions of euros spent on keeping gas prices for households under control, record inflation, which the ECB is fighting with interest rate hikes, a slowdown in the European economy and the threat of recession in the entire eurozone. Germany alone spent 18 billion euros at the end of July 2022 on measures to limit electricity and gas price increases. In December of that year, 22.7 billion euros were allocated for consumer benefits for energy supplies. The entire package of support measures is estimated at 200 billion euros. Even the economy of wealthy Germany cannot withstand such expenditure. At the end of August 2023, German Chancellor Olaf Scholz admitted to Bloomberg that Germany lacks the funds to subsidize electricity prices in the long term. According to forecasts by leading experts from the Institute of German Economics and the international consulting company Frontier Economics, published on the website of the authoritative analytical center Dezernat Zukunft, the current high energy prices can seriously threaten the economic situation in Germany. The study shows that if the German authorities fail to develop effective measures to reduce energy costs for industry and business, the German economy may lose up to 1.7 million jobs by 2030. This will inevitably lead to a decrease in the republic's gross domestic product by 1.7-4.5%. At the same time, even after the implementation of large-scale programs to switch to such a promising type of fuel as "green" hydrogen, electricity prices in Germany, according to experts, will exceed the world average by 30-65%[6]. A study conducted by the leading German Chamber of Industry and Commerce confirmed the concerns of the business community in Germany. 52% of companies negatively assess the impact of the energy transition on their activities due to rising costs and the likelihood of energy shortages. Analysts say that without a return to cheap Russian gas supplies, fuel and electricity prices in Germany are likely to remain extremely high, which would seriously harm the country's economic competitiveness. Hence, there are voices in Berlin about the need to repair the blown-up Nord Stream 1 and 2 gas pipelines[7].

Secondly, industry. In recent years, Europe has been deindustrialized. Industrial production fell by 20% in 2022 and by 10% in the first half of the comparable period in 2023, although it would seem that gas prices in 2023 are much more convenient (not $1,000-3,000 per thousand cubic meters, but only $400-500). This means that the European industry has reduced its production by almost a third. A number of industries in Europe have been closed, mainly energy-intensive chemical plants for the production of mineral fertilizers, and

[6] K. Surdyk, *UE i NATO wobec zagrożeń hybrydowych*, [in:] *Rzeczpospolita Polska w NATO i UE*, ed. Z. Nowak, Warszawa 2024, pp. 261-292.

[7] M. Kretschmer, From an interview with the Prime Minister of a German federal state Saksonia, Michael Kretschmer for "Wirtschaftswoche", 25-26.08.2023.

part of their production has been moved from Europe to the USA. In the United States, compared to Europe, there is a better investment climate and more favorable conditions for further work. As Bild writes (issue of August 21, 2023), as a result of restrictions on the import of Russian gas for the chemical industry, gas prices in Germany have increased by 40%, and the cost of producing mineral fertilizers by 150%. In this situation, "gas-intensive fertilizer production" turned out to be "unprofitable", and the supply of "Russian fertilizers to the EU", according to the industry, "increased fivefold over the year". Some experts believe that Russia treats the food crisis as a weapon. Previously, this was said about energy sources, and no one took food problems into account, especially at the EU level. Meanwhile, it was clear that Russia was preparing for war, as it stopped exporting fertilizers and developed its production capacities in the agri-food sector. In the meantime, Russia was developing this sector of the economy, becoming an exporter of food. Ukraine is also an exporter of food, and the war of these countries immediately affected the food situation in other countries[8].

Thirdly, finances. The Ukrainian conflict has also created certain threats to the finances of the European Union. Although in the sphere of finances, it is primarily the United States and Europe that are the attacking parties. In the geopolitical game with Russia, the West has used a financial weapon that is very painful for this country. It has blocked its currency reserves, mainly in dollars, but also reserves in euros, British pounds and yen. Russia's ability to make payments in these currencies has also been seriously limited, by disconnecting major Russian banks from the international SWIFT financial transaction system. In principle, after such radical steps, one could calmly watch the collapse of Russian finances, if not for the fact that very disturbing movements have begun in the global financial system, which may indicate that such actions by the West may be a "double-edged sword". It is expected that the war and the humanitarian crisis in Ukraine, the sanctions imposed on Russia and the risk of the conflict expanding - these are factors that will have a significant and multi-directional impact on the central banks and the entire banking sector of the European Union countries. Although the risks of banks in individual EU countries differ, we can identify a wide range of closely related threats[9]. These include: financial sanctions, legal and image risks, macroeconomic, market and credit risks related to high market uncertainty, as

[8] J. Kwieciński, V-ce President Pekao Bank, statement during the debate on „Krynica Forum '22 – Wzrost i Odbudowa", <https://www.rp.pl/wydarzenia-gospodarcze/artykul/37296281-wplyw-wojny-w-ukrainie-na-gospodarke> (25.10.2022).

[9] *Konsekwencje wojny w Ukrainie dla europejskiego sektora bankowego. Wpływ na banki centralne i cały sektor bankowy państw Unii Europejskiej*, <https://kpmg.com/pl/pl/home/insights/2022/04/artykul-konsekwencje-wojny-w-ukrainie-dla-europejskiego-sektora-bankowego.html> (22.04.2022).

well as the need for some banks to update their strategies and business models, especially in Eastern Europe. The coming months will be critical for understanding how events will unfold. Banks must ensure that they take appropriate preventive measures. It is difficult to predict how the crisis will evolve and what its ultimate impact on the Western economy and its banking sector will be. However, experts recommend that European banks in particular take the necessary steps to ensure resilience to various scenarios of economic development. In Poland, the war in Ukraine has caused a deterioration in the macroeconomic environment due to the impact of both supply and demand factors. Although the shock related to the crisis in Ukraine is not able to shake the foundations of the Polish banking sector, it may amplify existing tensions or weaknesses in the banking system. In particular, the greatest threat to the stability of the banking sector is the occurrence of many shocks in a relatively short horizon, generating losses in the banking system or negatively affecting the long-term ability of banks to generate profits.

A certain threat to the entire Western financial system, the Bretton-Woods system, based on the dollar, is the desire of Russia, but also China and other countries affected by Western sanctions, such as Iran or Venezuela, to conduct financial settlements bypassing Western currencies, and above all the main, world settlement currency, the US dollar. These countries are trying to convince their allies to settle in national currencies, and they themselves are starting to experiment with digital currencies, and even attempt to create a common currency, e.g. a common currency of the BRICS countries. The BRICS countries, led by Russia, are also examining the possibility of creating their own settlement system in foreign trade. Such a solution may be very profitable for these countries economically, but dangerous for Western countries from a political point of view, because it will make the BRICS countries independent of the will of Western politicians. It is to be an "independent settlement payment system based on the digital principles of blockchain". This settlement system was first discussed during the meeting of the finance ministers and central bank governors of the BRICS countries in Sao Paulo, Brazil, in 2024. A decision was made to prepare a report that will include a list of initiatives and recommendations in the field of financial settlements of the organization, including consideration of the possibility of creating a common settlement and payment platform BRICS Bridge. It is also worth noting that within the framework of financial cooperation in BRICS, special emphasis is placed on increasing the share of national currencies in mutual settlements and creating an independent, equally accessible financial infrastructure[10].

[10] *Finance ministers discuss BRICS Bridge digital currency payments*, February 28, 2024, <https://www.ledgerinsights.com/brics-bridge-digital-currency-payments/> (28.02.2024).

Needless to say, such initiatives, in which Russia actively participates, help to bypass the sanctions imposed on it and mitigate the effects of the economic war waged against this country.

BIBLIOGRAPHY:

1. *Finance ministers discuss BRICS Bridge digital currency payments*, February 28, 2024, <https://www.ledgerinsights.com/brics-bridge-digital-currency-payments/>
2. *Konsekwencje wojny w Ukrainie dla europejskiego sektora bankowego. Wpływ na banki centralne i cały sektor bankowy państw Unii Europejskiej*, <https://kpmg.com/pl/pl/home/insights/2022/04/artykul-konsekwencje-wojny-w-ukrainie-dla-europejskiego-sektora-bankowego.html>
3. Kretschmer M., From an interview with the Prime Minister of a German federal state Saksonia, Michael Kretschmer for "Wirtschaftswoche" 25-26.08.2023
4. Kukuła W., *Skutki wojny na Ukrainie – długoterminowe ryzyka dla globalnej motoryzacji*, <https://magazyn.cartrack.pl/wojna-na-ukrainie-konsekwencje-dla-motoryzacji/>
5. Kwieciński J., V-ce President Pekao Bank, statement during the debate on „Krynica Forum '22 – Wzrost i Odbudowa", <https://www.rp.pl/wydarzenia-gospodarcze/artykul/37296281-wplyw-wojny-w-ukrainie-na-gospodarke>
6. Movchan V., Research Director at the Institute of Economic Analysis and Policy Consulting in Kijev, statement during the debate on „Krynica Forum '22 – Wzrost i Odbudowa", <https://www.rp.pl/wydarzenia-gospodarcze/artykul/37296281-wplyw-wojny-w-ukrainie-na-gospodarke>
7. *Rynkowe skutki rosyjskiej inwazji na Ukrainę: reakcja UE*, <https://www.consilium.europa.eu/pl/policies/eu-response-ukraine-invasion/impact-of-russia-s-invasion-of-ukraine-on-the-markets-eu-response/>
8. Surdyk K., *Konflikt ukraiński w rozgrywkach geopolitycznych*, Warszawa 2017
9. Surdyk K., *UE i NATO wobec zagrożeń hybrydowych*, [in:] *Rzeczpospolita Polska w NATO i UE*, ed. Z. Nowak, Warszawa 2024

„Ante Portas – Security Studies”
2024, No. 21
DOI: 10.33674/1202422

Alika GUCHUA[1]
Georgia
Ketevan SHOSHIASHVILI[2]
Georgia

THE 2022-2024 RUSSO-UKRAINIAN WAR AND FOOD SECURITY POLICY

Abstract: *The aim of the paper is to determine the impact of the ongoing Russo-Ukrainian war on food security policy. What are the main challenges and threats that a number of states faced in terms of food security. The Russo-Ukrainian war had a significant impact on various processes in the world, among which an important place is given to food security policy. Because it took on both geopolitical and geoeconomic characteristics, which shifted the issue from a regional scale to a global format, along with other factors. As for the research methods, to obtain reliable information, we used: policy research analysis, content analysis and document analysis methods to analyze and describe the food security challenges arising from the Russo-Ukrainian war. The research process uses: “Political Realism Theory”, “Balance of Power Theory”, “Securitization Theory”. The effects of Russia’s destruction of Ukraine’s agriculture sector extend beyond global food insecurity, as Russia uses its own agricultural exports for influence in the Global South. Since Russia leverages its own agricultural exports to gain influence in the Global South, the consequences of its destruction of Ukraine's agriculture sector go beyond the world's food crisis. A significant part of the study was devoted to the analysis of the impact of armed conflicts and wars on food security in the context of the Russian-Ukrainian war and the discussion of this case. Attention is also paid to the global policy of food security and the political, economic and social factors influencing it. Among them, geopolitical and geoeconomic factors of food security are analyzed against the background of modern*

[1] Alika Guchua, PhD, Caucasus International University (Georgia), ORCID: 0000-0003-0347-9574, email: alika_guchua@ciu.edu.ge
[2] Ketevan Shoshiashvili, PhD, Caucasus International University (Georgia), email: qetevan.veliashvili@ciu.edu.ge

processes in the world. The article pays considerable attention to the role and importance of food security in ensuring global security.

Keywords: *food security, war, global food crisis, international security, Ukraine, Russia*

Introduction

In the modern era, the world is faced with a rather complex situation and reality regarding food security. The problem of food security is relevant for almost every country. It is worth noting that this problem is present in different doses and conditions in each country depending on its geographical location, the climate zone in which it is located, as well as the socio-political situation in a given state. However, there are also certain similarities that are important, since problems related to food security affect many countries, so it is a global problem, so this serious problem requires great attention from states and international organizations. The failure of the global food security system leads to loss of health and often to death. There are numerous cases of food counterfeiting, when counterfeit products are transported from country to country, which creates a health hazard. Among them is, to put it mildly, disregard for the law, which can lead to a dead end in political relations between two countries. Disagreements, tensions and deterioration of relations between countries will follow. Preventing such incidents and solving problems is of paramount importance today. Scientists, politicians and representatives of organizations working in the field of food security, and in particular food safety, in many countries of the world recognize that the main violations and problems in this area require urgent attention and timely solutions. Conflicts and hot spots around the world also have a significant impact on food security policy. The Russian-Ukrainian war, which began in 2022, has created a serious food problem for Ukraine and other states dependent on Ukrainian and Russian grain.

Food security is an integral part of national security and is its inevitable component. This phenomenon, in turn, is related to the fight against hunger and poverty in any country, and these two factors represent important challenges to national security. It can be said that these are asymmetric threats and challenges, the prevention and neutralization of which is precisely a component of national security.

Food security is influenced by factors that can be defined as internal or domestic political and economic challenges. These include the following factors: corruption and nepotism, food availability, significant dependence on imports, failure of economic reforms, environmental disasters, etc. As for

external factors, they can be manifested as global hunger, global epidemics, armed and military conflicts, food inflation at the global level, ecological and economic crises at the global level, etc. Both factors have a direct impact on the sustainability of food security and lead to the creation of high levels of vulnerability, both nationally and internationally.

In current international relations, food security has been identified as an inevitable component and an important factor in the geopolitical modeling of world political processes. Global initiatives have emerged, such as the "Global Alliance against Hunger and Poverty", founded by the leading actors of the global "South": Brazil, the Republic of South Africa, and also an intergovernmental association "African Union" with a global geopolitical mission and objectives.

Food security as part of the strategy of war

Military conflicts are one of the inevitable factors that can cause countries to suffer from food insecurity due to reduced agricultural productivity, increased food prices, and the deterioration of agricultural land and infrastructure. Farmland may become fallowed and abandoned as a result of reduced investment in agricultural management caused by military conflicts[3]. Russia's invasion of Ukraine and attacks on Ukraine's agricultural sector have had unprecedented, completely preventable effects on global food security, nutrition, and agricultural markets. The United States and other nations responded quickly and thoroughly. However, millions of people are experiencing worsening starvation as a result of the invasion, and humanitarian aid for those experiencing the most severe types of food poverty is being delayed[4].

Food access has long been a crucial factor in conflicts. It seems to be a key component of sieges as a military tactic, and military historians have studied how both armies and civilians have dealt with food shortages during conflicts. The global food system has changed over the past few decades, bringing with it new interdependencies that affect food security and preparation well beyond the front lines. Whether or not there is a clear plan to take advantage of food exports during a conflict, a conflict between two major food producers has an impact on societies all over the world, with potentially dire local

[3] Y. Ma, D. Lyu, K. Sun, S. Li, B. Zhu, R. Zhao, M. Zheng, K. Song, *Spatiotemporal Analysis and War Impact Assessment of Agricultural Land in Ukraine Using RS and GIS Technology*, "Smallholder Farming under External Shocks: New Perspectives and Solutions for Future Crises" 2022. <https://www.mdpi.com/2073-445X/11/10/1810> (12.10.2024).

[4] C. Welsh, *Russia, Ukraine, and Global Food Security: A One-Year Assessment. Center for Strategic and International Studies*, 2023, <https://www.csis.org/analysis/russia-ukraine-and-global-food-security-one-year-assessment> (14.10.2024).

repercussions[5]. Given the climate problem, it may be more crucial than ever to pay attention to food security. The global food system is both a contributor to and a danger to unsustainable living patterns, in addition to the consequences brought about by antagonist actors. Food and the food supply may be the primary security concern of the future due to the anticipated rise in the global population. This is especially true when food production declines in many parts of the world.

A familiar military strategy involving food is starvation as part of siege tactics. This strategy has very old records but seemed to vanish after the end of the Cold War. In recent years, however, Hägerdal (2020) notes that the tactic hasreappeared in relation to civil wars, and in particular urban warfare contexts. He arguesthat the militaries of Western democracies may face conflicts between the military utilityof starvation as a tactic and its political values. Warring parties may prevent the inter-national community from acting on such military strategies, and humanitarian organiza-tions may have trouble assisting civilians when a siege is complemented by heavybombing[6]. After a protracted time of no food, water, or electricity, the Russian capture of Mariupol in 2022 may have qualified as a siege because, at the very least, the troops and civilian population were compelled to evacuate. Because of the shooting and bombing, the international humanitarian community was unable to oversee long-term humanitarian bridges into the city.

There is a positive link between food security and stability. Conversely, especially in a globalized era, armed conflicts can be a key driver of food insecurity that affects regions beyond the battlefield; the food crises of the past decade have laid bare the systemic challenges in fending off food insecurity in conflict settings. These crises reveal why governments or belligerents lack either the capacity or the will to address them, and why humanitarian aid struggles to reach people in need[7]. The ongoing conflict between Russia and Ukraine has brought attention to fundamental flaws in global food security while also causing fresh food insecurity.

Armed conflicts make it more difficult for countries, families, and individuals to meet their food demands. Activities aimed at growing and harvesting, processing and transporting, and supplying and marketing food may be hampered by these conflicts. More precisely, conflicts can impact the ability of food systems and supply chains to operate effectively: production can

[5] A. Holmberg, *Food security in light of the war in Ukraine: food studiesmeets defence studies*, Taylor & Francis, "Defence Studies" 2024, Vol. 24, No. 4, <https://www.ifpri.org/blog/russia-ukraine-crisis-poses-serious-food-security-threat-egypt> (15.10.2024).

[6] A. Holmberg, *op. cit*.

[7] M. Behnassi, M. E. Haiba, *Implications of the Russia–Ukraine war for global food security*, "Nature Human Behaviour" 2022, <https://www.nature.com/articles/s41562-022-01391-x> (16.10.2024).

decrease because producers are involved in the conflict and cannot produce or escape the country; agricultural inputs can be disrupted on international markets; or military operations can destroy agricultural yields and water infrastructure. Due to the issue of food supply or their dwindling purchasing power, armed conflicts can also impact consumers' ability to obtain enough food. Such conflicts affect the ability of international food aid to meet growing food needs in times of crisis; they disrupt energy markets, which negatively impacts the purchasing power of importing countries; and they raise food prices on local and international markets, which negatively impacts low-income countries that import food. Therefore, any strategy employed throughout the conflict management process should take into account these food difficulties, which today represent a significant aspect of armed conflicts.

Russia's invasion of Ukraine serves as an example of how food security is affected by conflict. The effects of climate change will worsen this relationship because rising sea levels, rising temperatures, and more frequent hazards make this relationship worse. The combined effects of climate change and geopolitical conflict also make the situation of global food security worse than it has ever been.

The ongoing Russia-Ukraine war and food security policy

Ukraine is a major supplier of agricultural products, such as grains and sunflower oil, and is frequently referred to as the breadbasket of Europe. It is essential to provide for many countries' food needs. With prolonged disruption of agricultural production, distribution networks and trade routes, the continuing conflict in one of the most fertile countries in the world has exacerbated existing challenges and created new hurdles for ensuring access to food and improved socio-economic wellbeing for millions of people. The pain of the fighting extends far beyond Ukraine's borders[8].

Despite contributing a mere 2% to the global gross domestic product (GDP), Russia and Ukraine are notable producers and exporters of essential agricultural commodities, energy resources, and fertilizers[9]. Russia and Ukraine export 40% of the world's grain, making them major exporters. According to the United Nations, the COVID-19 pandemic and the Russia-Ukraine conflict have combined to cause the largest food catastrophe since World War II, with up to

[8] L. Emediegwu, *Update: how is the war in Ukraine affecting global food prices?*, "Prices & Interest Rates" 2024, <https://www.economicsobservatory.com/update-how-is-the-war-ukraine-affecting-global-food-prices> (19.10.2024).

[9] T. B. Hassen, B. E. Bilali, *Conflict in Ukraine and the unsettling ripples: implications on food systems and development in North Africa*, "Agriculture & Food Security" 2024, <https://agricultureandfoodsecurity.biomedcentral.com/articles/10.1186/s40066-024-00467-3> (20.10.2024).

1.7 billion people living in poverty and hunger, a number that is currently at an all-time high. About 30% of wheat and barley are supplied by Russia and Ukraine, resulting in a concentrated structure in the global grain market. Their contribution to the wheat market is vital in specific global markets, principally in the Middle East and North Africa (MENA) region, where wheat is a fundamental food source. Russia and Ukraine are important contributors to barley's global production and export, accounting for 20% of the total output, and are the third and fourth exporters[10]. A total of 36 countries, including some of the world's most vulnerable and impoverished, import more than half their wheat from them. Because of this, the conflict between Ukraine and Russia quickly derailed global food supplies and led to high prices. It pushed millions into extreme poverty and worsened hunger and malnutrition and there were 222 million people in 53 countries and territories suffering from severe food crises and in need of emergency assistance[11]. Implications for regional and global food security will be far-reaching, with 41.5 million ha of highly fertile land larger than the agricultural area of France (18 million ha), Germany (12 million ha) and Poland (11 million ha) combined, given Ukraine's traditional role as a breadbasket and a main exporter of wheat and sunflower oil. After the start of the war, grain prices rose well above the levels experienced in the 2007/08 food crisis, highlighting agriculture's geostrategic role[12].

The ongoing Russian-Ukrainian war of 2022-2025 has not only changed the agenda of these two countries, but also created serious problems for the world order in terms of food security. Ukraine, which is considered one of the largest suppliers of grain to the world market, faced the problem of exporting its agricultural products as a result of the war. Here, the so-called "domino principle" worked - food shortages arose in countries that were largely dependent on Ukrainian grain. In response to this crisis, in 2022, at the initiative of the United Nations and the Republic of Turkey, an agreement was approved, the purpose of which was to restore and ensure the transportation of Ukrainian grain - wheat, which in itself implies ensuring global food security. It was signed in Istanbul on 22 July 2022, and was at first valid for a period of

[10] *Ibidem*.

[11] F. Lin, X. Li, N. Jia, F. Feng, H. Huang, J. Huang, Sh. Fan, P. Ciais, X-P. Song, *The impact of Russia-Ukraine conflict on global food security*, "Global Food Security" 2023, <https://www.sciencedirect.com/science/article/pii/S2211912422000517> (22.10.2024).

[12] K. Deininger, D. A. Ali, N. Kussul, A. Shelestov, G. Lemoine, H. Yailimova, *Quantifying war-induced crop losses in Ukraine in near real time to strengthen local and global food security*, "Food Policy" 2023, <https://www.sciencedirect.com/science/article/pii/S0306919223000167> (24.10.2024).

120 days[13]. However, this landmark agreement, designed to ensure humanitarian and global food security, turned out to be part of an information war, a propaganda tool and, as a result, almost acquired a diplomatic lever for managing global reactions and crises. In February 2022, the Russian Federation's military aggression in Ukraine, which escalated into a full-scale war, not only undermined regional security and had a serious impact on relations between the warring countries, but also brought global security issues to the forefront. An agenda that covers virtually all areas of international relations around the world, including the global economy and trade, as well as agricultural supplies.

In the first days of hostilities, land transportation from Ukraine was seriously disrupted and agricultural exports along the Black Sea corridor virtually ceased. As a result, Ukraine, the world's largest wheat producer and exporter, was unable to fulfill its obligations. This led to food and feed shortages in regions and countries dependent on Ukrainian grain. There is no doubt that the conflict has exacerbated the vulnerability of several countries, particularly in the Global South. It threatens their food security with potentially serious humanitarian consequences, especially in regions that are most dependent on Russian and Ukrainian food exports, such as Middle East and North Africa (MENA) region[14]. Being the world's most water-scarce region, the MENA area is heavily dependent on food imports. It is also regarded as one of the areas most susceptible to climate change worldwide. Furthermore, political instability, fragility, and ongoing conflicts are common in the region (see, for example, Syria, Yemen, Somalia, and Sudan), which leads to a large number of refugees being housed by neighboring countries and widespread food shortages. The situation was particularly difficult for less developed countries in Middle East and Asia, where their populations faced the threat of famine and humanitarian catastrophe. The problem required an immediate response, and to overcome the crisis, the foundation of the "Black Sea Grain Initiative" was laid with the participation of important players of the world order.

This platform, which has a purely humanitarian content, is aimed at creating safe routes and routes for the transportation of agricultural products in the Black Sea basin, which would allow transport structures to supply Ukrainian grain to the world market.

The "Black Sea Grain Initiative" as a purely humanitarian and economic agreement has become an integral part of political propaganda and political insinuations. The "agreement" was turned into a tool of propaganda warfare by

[13] C. Steuer, O. Rieker, *Food Security in the Context of the War in Ukraine*, Ústav mezinárodních vztahů, Praha 2023, <https://www.iir.cz/food-security-in-the-context-of-the-war-in-ukraine> (26.10.2024).
[14] T. B. Hassen, B. E. Bilali, *op. cit*.

the warring countries: Russia and Ukraine, as well as their allied forces. Both sides, including neutral countries, voiced their versions and tried to create established visions of the agreement to advance their broader interests and goals, or at least to strengthen their global influence.

The second initiative was to control the current food crisis. The Food Agriculture Resilience Mission (FARM), a partnership between France and the UN World Food Programme, aimed to help the nations most affected by the crisis by promoting sustainable agriculture and guaranteeing that the most vulnerable nations received agricultural commodities at a fair price. It accomplishes this by emphasizing the effectiveness of agricultural markets, encouraging locally produced food that is sustainable, and working with the private sector to distribute food surpluses to the nations who need them the most.

At the European level, important decisions have been taken, including those for providing emergency financial help and 1.5 billion euros to support the development of sustainable agriculture in the Eastern and Southern neighborhood. Most notably, the EU created "solidarity lanes" as alternative logistical routes for transporting cargo shipments of grain to the Black Sea region by rail, road, and river. 60% of the Ukrainian grain product was exported through the European "solidarity corridors," and the rest of it through the Black Sea Grain Initiative. Moreover, the EU allocated 7.7 billion euros for food security in the period 2021–2024[15].

Russia's withdrawal from the Black Sea grain deal in July 2023 and any further reduction of Ukrainian grain exports are likely to have serious implications for both Ukraine's agricultural sector and economy and for food security far beyond Europe's borders, driving up food prices and hindering humanitarian agencies' ability to respond to food crises[16]. In addition to increasing market volatility, Russia's decision to leave the Black Sea Grain Initiative has decreased the world's grain supply at a crucial moment for those who are most in need worldwide. In an obvious attempt to weaken Ukraine's capacity to export food to the rest of the world, Russia has also targeted Ukrainian civilian grain and port facilities in a methodical manner. It will take years to undo Russia's activities, which have long harmed Ukraine's agriculture industry, which has been so important to the world's food supply. However, Ukraine's food production and exporting capacities have both been affected by the war. Widespread landmine and explosive remnants of war (ERW)

[15] C. Steuer, O. Rieker, *op. cit*.

[16] M. Riquier, H. Garbino, *War in the breadbasket: Landmines and food security in Ukraine*, Stockholm International Peace Research Institute 2024. <https://www.sipri.org/commentary/blog/2023/war-breadbasket-landmines-and-food-security-ukraine> (02.11.2024).

contamination could render vast tracts of agricultural land unusable, possibly for years, endangering food security both at home and abroad. Important issues regarding the priority and regulation of humanitarian mine action should be taken into consideration by the Ukrainian government as it prepares a new mine action policy. Over one third of Ukraine is suspected to be contaminated with landmines and other explosive hazards, and nearly 6.5 million acres of the country's farmland has been adversely impacted by the Russia's aggression, according to Ukraine's Ministry of Economy[17]. Millions of citizens' livelihoods are in danger due to widespread mine pollution, which also hurts the economy by lowering Ukraine's agricultural output. The United States is dedicated to assisting Ukraine provide safe access to arable land and return that land to communities for long-term productive use, as it is the largest humanitarian demining assistance contributor to Ukraine. The ongoing presence of landmines and other explosive dangers left by Russian forces in Ukraine's prime agricultural land poses a serious threat to food security, investment, and human life.

Ukraine's ability to produce and export has already been impacted by Russian strikes that have damaged its farms, storage facilities, arable lands, and agricultural equipment. This, together with Russia's move to prohibit fertilizer exports, is probably going to keep driving up food costs. In light of this, the IMF is calling on governments and donors to provide assistance for the most disadvantaged, guarantee the effectiveness of the agricultural market, and eliminate detrimental subsidies. There is no longer space for structural reforms in those nations (such as Egypt and Tunisia) who are already having trouble with the rise in their foreign debt brought on by the spike in wheat prices. They could get through the current crisis with the aid of a debt reduction.

The conflict in Ukraine has disrupted vital supply networks and increased expenses for struggling businesses attempting to ship goods globally, which are subsequently passed on to customers. Maintaining unrestricted trade in food, fuel, and fertilizer is essential to reducing the rise in food insecurity in Ukraine and around the world. This involves protecting food supply chains and agricultural output in general, as well as the infrastructure and storage facilities used to transport foodstuffs—particularly grains—out of the nation. To guarantee that food produced in Ukraine can freely travel to the rest of the globe, the blockade of Ukrainian ports must end right away.

More prosperous economies appear to be successful in adapting to and mitigating the food impact of the war in Ukraine. But many developing and emerging economies are still grappling with the food crisis problem. Just like

[17] R. Yang, *Improving Food Security in Ukraine Through Demining*, U. S. Department of State 2024, <https://www.state.gov/improving-food-security-in-ukraine-through-demining/> (04.11.2024).

Covid-19, the issue of food insecurity should be a global concern, as 'hunger in one country is a threat to other countries'[18]. In order to help struggling nations, coordinated measures must be done. After all, one of the Sustainable Development Goals (SDG 2) of the UN is to eradicate hunger and malnutrition worldwide. This in turn is a critical component in the fight for global food security and a shared global challenge that can only be addressed through international collaboration across countries, organizations and sectors, and through innovation in science, technology and more open sharing of data, methods and expertise[19]. Global conflicts pose a serious risk to achieving this goal.

The war in Ukraine has also emphasized the interconnection of food chains and food systems, as well as the necessity for more international scientific collaboration and knowledge-sharing to address the complex and interdependent challenges facing the agri-food sector[20]. Through this partnership, nations can share best practices, gain knowledge from each other's experiences, and develop cooperative solutions to global environmental and food security issues. The variations in impact levels and channels among nations and regions must also be taken into account by policymakers. They must acknowledge the interconnectivity of the global food system while utilizing context-specific approaches tailored to the unique opportunities and difficulties faced by each location.

Conclusion

Based on the above, modern international security challenges, such as climate change, conflicts, conventional wars (on the example of the Russia-Ukraine war), international terrorism, illegal migration, illegal arms transit and organized criminal groups based on them, global-level technogenic disasters, drought, entomological warfare, during which insects are used against enemy crops, therefore, it poses a threat to agriculture, etc. are directly correlated with ensuring food security and vulnerability.

The war t in Ukraine serve as examples of how inadequate security and defense policy understanding of the factors influencing food security is. A conflict between two major food producers impacts societies all across the world, regardless of whether there is a clear plan to take advantage of food

[18] L. Emediegwu, *op. cit.*

[19] I. Becker-Reshef, C. Justice, B. Barker, M. Humber, F. Rembold, R. Bonifacio, M. Zappacosta, M. Budde, T. Magadzire, C. Shitote et al., *Strengthening agricultural decisions in countries at risk of food insecurity: The GEOGLAM Crop Monitor for Early Warning*, "Remote Sens of Environ" 2020, <https://www.sciencedirect.com/science/article/pii/S0034425719305735> (12.11.2024).

[20] T. B. Hassen, B. E. Bilali, *op. cit*.

security during a conflict. Many people have already died in the fight. Reducing the number of people affected by food shortages should be a top priority for decision-makers everywhere.

First, a significant vulnerability in the global food system is the concentration of power. Second, many nations' reliance on food imports raises the possibility of future conflict dynamics. Third, the challenges of managing the global food system must be considered in attempts to direct food preparation within defense policy frameworks. Fourth, the conflict in Ukraine has highlighted the crucial role that the international community – exemplified by the FAO – plays in providing nations with food-related assistance.

In the end, we need to change the way we handle conflict and its effects. The issue of food security is a vital national security interest and should be a focus of attention for countries around the world. The effects of war, such as migration, supply chain disruptions, and food shortages, are no longer limited to a single location. A issue in one area can swiftly turn into a worldwide disaster since the whole community is intricately linked and only gets more so. The only way to solve the problem is to address the root causes of food insecurity.

Ensuring food security should meet the interests of all states, which can be achieved by avoiding wars, conflicts and destabilization of the situation in the world. And the resources spent on these processes should be directed to the creation of a sustainable food security policy that will eliminate food shortages, effectively manage the negative processes caused by climate change and provide the world's population with food to meet its growing needs. In this general policy, along with states, a decisive role is given to regional and international organizations, whose work should be more pragmatic and effective.

BIBLIOGRAPHY:

1. Abay K., Abdelfattah L., Breisinger C., Glauber J., Laborde D., *The Russia-Ukraine crisis poses a serious food security threat for Egypt*, "Communities & Collections" 2022, <https://doi.org/10.2499/9780896294394_24>
2. Balma L., Heidland T., Jävervall S., Mahlkow H., Mukasa A. N. et al., *Long run impacts of the conflict in Ukraine on grain imports and prices in Africa*, "African Development Review" 2024, <https://onlinelibrary.wiley.com/doi/10.1111/1467-8268.12745?af=R>
3. Becker-Reshef I., Justice C., Barker B., Humber M., Rembold F., Bonifacio R., Zappacosta M., Budde M., Magadzire T., Shitote C. et al., *Strengthening agricultural decisions in countries at risk of food*

insecurity: The GEOGLAM Crop Monitor for Early Warning, "Remote Sens of Environ" 2020, <https://www.sciencedirect.com/science/article/pii/S0034425719305735>
4. Behnassi M., Haiba M. E., *Implications of the Russia–Ukraine war for global food security*, "Nature Human Behaviour" 2022, <https://www.nature.com/articles/s41562-022-01391-x>
5. Bilali H. E., Hassen T. B., (2024) *Disrupted harvests: how Ukraine – Russia war influences global food systems – a systematic review*, "Policy Studies" 2024, <https://www.tandfonline.com/doi/full/10.1080/01442872.2024.2329587#abstract>
6. Deininger K., Ali D.A., Kussul N., Shelestov A., Lemoine G., Yailimova H., (2023) *Quantifying war-induced crop losses in Ukraine in near real time to strengthen local and global food security*, "Food Policy" 2023, <https://www.sciencedirect.com/science/article/pii/S0306919223000167>
7. Dongyu Q., (2022) *New Scenarios on Global Food Security based on Russia-Ukraine Conflict*, "Food and Agriculture Organization of the United Nations" 2022, <https://www.fao.org/director-general/news/news-article/en/c/1476480/>
8. Emediegwu L., *Update: how is the war in Ukraine affecting global food prices?* "Prices & Interest Rates" 2024, <https://www.economicsobservatory.com/update-how-is-the-war-ukraine-affecting-global-food-prices>
9. Glauber J., Laborde D., Mamun A., (2022) *From bad to worse: how Russia-Ukraine war-related export restrictions exacerbate global food insecurity*, IFPRI is a CGIAR Research Center 2022, <https://www.ifpri.org/blog/bad-worse-how-export-restrictions-exacerbate-global-food-security/>
10. Hassen T. B., Bilali B. E., *Conflict in Ukraine and the unsettling ripples: implications on food systems and development in North Africa*, "Agriculture & Food Security" 2024, <https://agricultureandfoodsecurity.biomedcentral.com/articles/10.1186/s40066-024-00467-3>
11. Holmberg A., (2024) *Food security in light of the war in Ukraine: food studiesmeets defence studies*, Taylor & Francis, "Defence Studies" 2024, Vol. 24, No. 4, <https://www.tandfonline.com/doi/epdf/10.1080/14702436.2024.2378793?needAccess=true>
12. https://www.ifpri.org/blog/russia-ukraine-crisis-poses-serious-food-security-threat-egypt
13. Lang T., McKee M., (2022) *The reinvasion of Ukraine threatens global food supplies*, "Bmj-Br Med J", <https://www.bmj.com/content/376/bmj.o676.full>

14. Lin F., Li X., Jia N., Feng F., Huang H., Huang J., Fan Sh., Ciais P., Song X-P., (2023) *The impact of Russia-Ukraine conflict on global food security*, "Global Food Security" 2023, <https://www.sciencedirect.com/science/article/pii/S2211912422000517>
15. Ma Y., Lyu D., Sun K., Li S., Zhu B., Zhao R., Zheng M., Song K., (2022) *Spatiotemporal Analysis and War Impact Assessment of Agricultural Land in Ukraine Using RS and GIS Technology*, "Smallholder Farming under External Shocks: New Perspectives and Solutions for Future Crises", <https://www.mdpi.com/2073-445X/11/10/1810>
16. Riquier M., Garbino H., (2024) *War in the breadbasket: Landmines and food security in Ukraine*, Stockholm International Peace Research Institute 2024, <https://www.sipri.org/commentary/blog/2023/war-breadbasket-landmines-and-food-security-ukraine>
17. Steuer C., Rieker O., *Food Security in the Context of the War in Ukraine*, Ústav mezinárodních vztahů Praha 2023, <https://www.iir.cz/food-security-in-the-context-of-the-war-in-ukraine>
18. Welsh C., *Russia, Ukraine, and Global Food Security: A One-Year Assessment*. Center for Strategic and International Studies 2023, <https://www.csis.org/analysis/russia-ukraine-and-global-food-security-one-year-assessment>
19. Yang R., (2024) *Improving Food Security in Ukraine Through Demining*, U. S. Department of State 2024, <https://www.state.gov/improving-food-security-in-ukraine-through-demining/>

„Ante Portas – Security Studies”
2024, No. 21
DOI: 10.33674/1202420

Victoria BEVZIUC[1]
Moldova
Svetlana CEBOTARI[2]
Moldova

CYBER ATTACKS – RUSSIAN FEDERATION'S MECHANISM OF INFLUENCE IN UKRAINE

Abstract: *Currently, the international community is facing a hybrid conflict in Ukraine, where traditional and cyber weapons are being used at the same time. The big surprise of the Russian invasion was the apparent absence of a major cyber war. In addition to physical attacks on Ukraine, Moscow has resorted to launching cyber-attacks. For years, cyberspace has been considered a space where warfare can take place beyond space cyberspace has been considered a space where warfare can take place beyond land, water, or airspace. Since then, a multitude of cyber-attacks on Ukrainian infrastructure and its allies have been observed, of different types and with different objectives. This article highlights the main aspects of the cyber-attacks launched by the Russian Federation on Ukraine. Moreover, this article shows how the Ukrainian war may change the traditional parameters of international conflicts.*

Keywords: *threat, cyber security, cyber war, cyber attack, Russia, Ukraine, hackers*

Introduction

The presence of a high-intensity war on the European territory has marked the use of cyberspace as a battlefield between the Russian Federation and the West, including the Russian Federation and Ukraine. The cyber attacks have

[1] Victoria Bevziuc, PhD, Moldova State University, ORCID: 0000-0001-9189-641X, email: victoriabevziuc@yahoo.ro
[2] Svetlana Cebotari, PhD, DSc, Moldova State University, ORCID: 0000-0001-9073-104X, email: svetlana.cebotari11@gmail.com

now become an essential element of conflicts in the modern era, as demonstrated by the actions of both state and non-state actors in the cyber domain during the Russo-Ukrainian war[3].

According to the military theories, alongside the sea, air, land, and space domains, the cyber space is designated as the fifth domain of warfare. Today, we are witnessing a significant expansion of this fifth domain, with a multitude of cyber attacks being observed targeting the Ukrainian infrastructure and its allies, of various types and with different objectives.

For years, cyberspace has been considered a realm where warfare can occur beyond land, sea, or space domains, with a multitude of cyber attacks observed against Ukrainian infrastructure and its allies, of various types and with different objectives. Thus, Russia's invasion of Ukraine has altered both the real and virtual worlds. However, this moment is not a new one, as the current war stems from the prolonged Russo-Ukrainian conflict that began in 2014, characterized by Russian cyber attacks on critical Ukrainian infrastructure[4].

Conceptual distinctions between the terms "cyber warfare" and "cyber attack"

In today's increasingly digital world, cyber warfare is no longer a futuristic concept; it represents a real and significant threat to the national security and the interests of a nation[5]. Although some researchers consider cyber warfare equivalent to cyber attacks, there is a significant difference between these two terms. According on the theses put forth in 2009 by Martin Libicki, an expert on cyber warfare issues, in a report he wrote for the US Air Force, he presented a definition of "cyber warfare". Libicki considers cyber warfare as a directed and individualized war, not involving "real" or physical war, but rather a virtual one. Libicki mentions that "cyber warfare will play an important role in the future." Additionally, the author considers cyber warfare as possibly part of special warfare and focused on the use of so-called "soft power"[6]. For Libicki,

[3] *Dimensiunea cibernetică a conflictului Rusia – Ucraina – Desluşirea primei etape*, <https://dnsc.ro/citeste/dimensiunea-cibernetica-conflictului-rusia-ucraina-deslusirea-primei-etape> (12.09.2024).

[4] A. Gavrila, *La gran ciberguerra de Ucrania que no ocurrió*, <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO99_2022_ADAGAV_Ucrania.pdf> (12.09.2024).

[5] J. Mackay, *Cyber warfare: ¿Qué es la guerra cibernética?*, <https://www.metacompliance.com/es/blog/security-awareness-training/what-is-cyber-warfare> (20.04.2024).

[6] D. Trifunović, Z. Bjelica, *Cyber war – trends and technologies*, <https://www.researchgate.net/publication/349942064_Cyber_War_-_Trends_and_Technologies> (19.94.2024).

the cyber warfare is the systematic use of information, messages, etc., to attack information systems[7].

Analyzing the specifics of warfare, R. Guedes considers a "cyber warfare" as a form of conflict that takes place in the virtual space, where weapons are electronic devices, and the main objective is the control or destruction of information systems, communication networks, and critical infrastructure. This type of warfare can be conducted by governments, terrorist organizations, hacker groups, or individuals and can have devastating consequences for society, from economic damage to national security risks. The cyber warfare presents unique challenges compared to other forms of conflict due to its transnational and anonymous nature[8]. Additionally, a cyber warfare is used to destabilize a country by attacking critical infrastructure, such as national power grids, financial markets, or military databases. The damage resulting from such a large-scale attack could be devastating[9].

The cyber warfare exists in both the military and information domains, referring to the conduct of military operations based on informational principles. This involves disrupting or destroying information and communication systems. It also entails attempting to learn everything about the adversary while simultaneously reducing their attempts to learn too much about you. The cyber warfare is similar to traditional armed conflict, with differences lying in the environment of engagement - virtual - and the means through which it is conducted - networks and ICT (Information and Communication Technology) tools. Like other forms of warfare, the purpose of cyber warfare is to achieve certain interests - political, territorial, economic, or ethnic - by affecting the adversary's decision-making capacity, both politically and militarily, through operations in computer networks[10].

Three types of operations in computer networks can be distinguished: attacks - operations designed to disrupt, impede, degrade, or destroy information residing in computers or networks or even enemy computers and networks; espionage - gathering data and information from the adversary's computers through ICT means; defense - taking all necessary measures to protect one's own ICT means and infrastructure against the opponent's attacks

---

[7] M. C. Libicki, *Cyberwar as a Confidence Game*, <https://www.jstor.org/stable/26270514?seq=8> (19.09.2024).

[8] R. Guedes, *Guerra Cibernética: Tipos, Armas, Objetivos y Ejemplos de Guerra Tecnológica*, <https://ciberprisma.org/2023/05/10/guerra-cibernetica-tipos-armas-objetivos-y-ejemplos-de-guerra-tecnologica/> (19.09.2024).

[9] *Cyber warfare: ¿Qué es la guerra cibernética?*, <https://www.metacompliance.com/es/cyber-security-terminology/cyber-warfare> (19.09.2024).

[10] D. Trifunović, Z. Bjelica, *Cyber war – trends and technologies*, https://www.researchgate.net/publication/349942064_Cyber_War_-_Trends_and_Technologies> (20.09.2024).

and espionage. Thus, at a conceptual level, cyber attacks cover only a small portion of the total operations in computer networks[11].

Richard A. Clarke defines cyber warfare as actions sponsored by a nation-state to penetrate the networks or computers of other nations with the aim of causing damage or sabotage[12].

As in conventional warfare, the primary objective of cyber warfare is to weaken the country by undermining social cohesion, political stability, and military and industrial capacity. Although the boundaries between cyber warfare, cybercrime, and cyber terrorism may be blurred, cyber warfare is not primarily motivated by economic gain and is committed by agents affiliated with a country. The cyber warfare can include attacks against[13]:

- civil infrastructures, such as power grids or traffic management systems;
- financial entities, such as banks and credit unions;
- military installations, contractors, and other national security institutions;
- private citizens of the affected country.

Unlike the term "cyber warfare," the term "cyber attack" refers to any intentional effort to steal, expose, modify, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system, or digital device[14]. Referring back to J. Mackay's thesis, a cyber attack represents an operation conducted in computer networks aimed at disrupting, impeding, degrading, or destroying information present in enemy computers and networks[15]. The cyber attacks or the deliberate paralysis or destruction of enemy networks represent one of the numerous tools within military missions. A cyber attack is an elaborate hacking attack meant to undermine the computer security system. This type of attack can be considered a modern form of aggression, given the severity of its consequences comparable to an armed act[16].

A cyber attack represents any intentional effort to steal, expose, modify, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system, or digital device. In today's connected digital

---

[11] J. Mackay, *Cyber warfare: ¿Qué es la guerra cibernética?*, <https://www.metacompliance.com/es/blog/security-awareness-training/what-is-cyber-warfare> (19.09.2024).

[12] <https://www.cisco.com/c/dam/global/es_mx/products/pdfs/58-60-bridge.pdf> (19.09.2024).

[13] O. Buxton, *Ciberguerra: tipos, ejemplos y cómo protegerse*, <https://www.avast.com/es-es/c-cyber-warfare> (19.09.2024).

[14] *¿Qué es un ataque cibernético?*, <https://www.ibm.com/mx-es/topics/cyber-attack> (19.09.2024)

[15] James Mackay, *op. cit.*

[16] D. Arman, *Atacul cibernetic-o nouă formă de agresiune în dreptul internațional*, <https://ibn.idsi.md/sites/default/files/imag_file/28-31_23.pdf> (19.09.2024).

landscape, cybercriminals use sophisticated tools to launch cyber attacks. The cyber attacks come in various forms through computer networks and systems[17]:

- Malware or malicious software disguises itself as an email attachment or trusted program (e.g., encrypted document or file folder) to exploit viruses and allow hackers to penetrate a computer network. This type of cyber attack often disrupts an entire IT network. Some examples of malware include Trojans, spyware, worms, viruses, and adware;
- Distributed Denial of Service (DDoS) attacks involve multiple compromised computer systems attacked by hackers targeting a website or network and denying user activity on that website or network. For example, hundreds of pop-up windows, ads, and even a crashing website can contribute to a DDoS attack on a compromised server;
- Phishing is the act of sending fraudulent email messages on behalf of reputable companies. Hackers use phishing to gain access to data in a personal or corporate network;
- A SQL injection attack is where a cybercriminal exploits software, taking advantage of applications (e.g., LinkedIn, Target) to steal, delete, or gain control over data;
- Cross-Site Scripting (XSS) is the attack where a cybercriminal sends a link to a website that launches spam or is "script-injected," and it opens, delivering personal information to that cybercriminal;
- Botnet attacks involve multiple computers, typically from a private network, infected with viruses and other forms of malicious software, such as pop-up messages or spam;
- Ransomware is a type of malicious software or malware that threatens a victim by destroying or blocking access to critical data or systems until a ransom is paid.

Thus, if cyber warfare is a form of conflict conducted in the virtual space, carried out through electronic devices to pursue political, territorial, economic, or ethnic interests, as well as to impose the control or destruction of information systems by affecting communications networks and critical infrastructure of the adversary through operations, cyber attack represents an operation, a mechanism through which cyber warfare is carried out.

The impact of cyber attacks by the Russian Federation on Ukraine

There is a need to analyze cyber attacks during the conflict, for a better understanding of the impact of the Russo-Ukrainian war on security, especially

[17] *¿Qué es un ataque cibernético?*, <https://www.ibm.com/mx-es/topics/cyber-attack> (20.09.2024).

on cybersecurity, starting from the day of invasion (February 24, 2022)[18]. Thus, over two years since the emergence of the war, conditioned by the unjustified invasion of Ukraine by the Russian Federation on February 24, 2022, one of the threats added to humanitarian, political, or economic security is cybersecurity. It is noteworthy that the first signs of Russia's invasion into Ukraine appeared in cyberspace[19], looking back at the events in Ukraine. Russia initiated its war against Ukraine on February 24, 2022, but Russian cyber attacks against Ukraine have persisted since Russia's illegal annexation of Crimea in 2014, intensifying even before the 2022 invasion.

The evolution of cyber attacks is determined by the launch of the Russian military operation against Ukraine. Many researchers even agree that the first offensive in the Russo-Ukrainian war was cyber in nature and began at least a month before the emergence of physical warfare. Therefore, we can mention that as early as January 2022, the Ukrainian government faced DDoS (Distributed Denial of Service) cyber attacks launched by the Russian Federation against 70 government websites. Some of these attacks issued a warning to Ukrainians to "prepare for the worst." Thus, analyzing the war in Ukraine, it is noteworthy that Russian intervention in Ukraine was accompanied by large-scale operations not only in land and space domains but also in cyberspace even before February 24, 2022. Additionally, several security experts assert that they observed attacks against Ukrainian information systems[20] just hours before the bombardments launched by the Russian Federation against Ukraine. A series of DDoS attacks were launched against the websites of banks and Ukrainian government departments, rendering them inaccessible[21] with Kiev officially recording over 2,000 cyber attacks from Moscow[22].

Starting from December 12, 2022, cyber attacks by Russian hackers disrupted services provided by Ukraine's largest telecommunications operator

---

[18] *Dimensiunea cibernetică a conflictului Rusia – Ucraina - Deslușirea primei etape*, <https://dnsc.ro/citeste/dimensiunea-cibernetica-conflictului-rusia-ucraina-deslusirea-primei-etape> (12.09.2024).

[19] *Rusia coordina ciberataques en Ucrania, según Microsoft*, <https://www.dw.com/es/rusia-coordina-ataques-cibern%C3%A9ticos-y-militares-en-ucrania-seg%C3%BAn-microsoft/a-61615216> (12.09.2024).

[20] C. Blanc-Rolin, *Conflit Russie-Ukraine: la guerre est aussi cyber*, <https://www.dsih.fr/article/4608/conflit-russie-ukraine-la-guerre-est-aussi-cyber.html> (12.09.2024).

[21] *5 amenințări asupra securității cibernetice a statelor europene în contextul războiului ruso-ucrainean*, <https://bit-sentinel.com/ro/5-amenintari-asupra-securitatii-cibernetice-a-statelor-europene-in-contextul-razboiului-ruso-ucrainean/> (12.09.2024).

[22] J. C. de Santos, *Ucrania | La realidad ha dejado a la guerra cibernética en un segundo plano*, <https://es.euronews.com/2023/02/22/ucrania-la-realidad-ha-dejado-a-la-guerra-cibernetica-en-un-segundo-plano> (12.09.2024).

for approximately 24 million users for several days. According to statements from Illia Vitiuk, the head of the cybersecurity department at the Security Service of Ukraine (SBU), the cyber attacks caused "disastrous" damage, wiping out "almost everything," including thousands of virtual servers and PCs. Vitiuk describes this attack as the first example of a destructive cyber attack that "completely destroyed the core of a telecommunications operator" such as Kyivstar. Kyivstar is the largest of the three major telecommunications operators in Ukraine, and there are approximately 1.1 million Ukrainians living in towns and small villages where there are no other providers.

Additionally, according to SBU estimates, hackers stole personal information to track phone locations and intercept SMS messages, as well as stole Telegram accounts. The cyber attack on Kyivstar hastened Ukrainian citizens to obtain other SIM cards, creating long queues. ATMs using Kyivstar SIM cards for internet stopped working, and the air raid siren - used during missile and drone attacks - did not function properly in some regions. However, according to I. Vitiuk's statements, the attack did not have a significant impact on the Ukrainian army, which did not rely on telecommunications operators and used other "algorithms and protocols".

The cyber attack on Kyivstar was carried out by Sandworm, a Russian military intelligence cyber warfare unit that infiltrated a Ukrainian telecommunications operator. Additionally, cyber attacks by Sandworm were supported by the affiliated group called Solntsepyok, also responsible for the attack. Similarly, Sandworm was behind the cyber attacks on Ukraine's power grid in 2017 and the NotPetya malware operation[23].

For the conduct of a cyber war, which has both defensive and offensive characteristics, multiple methods of operation are used, as highlighted by Yannick Chatelain: "Both through the use of cyber propaganda and through DDoS attacks that aim to saturate a server or render a website unavailable, or even through data destruction by malicious software"[24]. The Russian invasion of Ukraine has led to the emergence of the first cyber war in history. The Russo-Ukrainian war is not only taking place on the ground; it also extends into cyberspace. Thus, according to research conducted by Yannick Chatelain, a professor at the Grenoble School of Management and a specialist in digital technology, we are currently witnessing the confrontation with the first cyber war of international dimensions[25].

---

[23] T. Balmforth, *Exclusive: Russian hackers were inside Ukraine telecoms giant for months*, <https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/> (12.09.2024).

[24] *Guerre en Ukraine: Pourquoi parle-t-on d'une cyberguerre*?, <https://guardia.school/le-lab/guerre-en-ukraine-pourquoi-parle-t-on-dune-cyberguerre.html> (12.09.2024).

[25] *Ibidem*.

We are currently witnessing the unfolding of a "cyber war", analyzing Russia's attacks on Ukraine, This is also the opinion of Major General Jürgen Setzer of the Cyber and Information Domain Command (KdoCIR) of the Bundeswehr when referring to Russia's attacks in the war against Ukraine. According to Setzer's opinion, governments' activities can be paralyzed or weakened through other means such as disinformation, fake news, and cyber attacks on vital infrastructure such as power grids, roads, railways, or hospitals. In this way, the objectives set by adversaries could be achieved "without resorting to weapons." However, the real dimension of the virtual war in Ukraine is unclear for a simple reason: "it is very difficult to establish the limits, the boundaries of cyberspace," Setzer explains. In other words, the virtual attacks are usually invisible at first, but their consequences can be immediate. On the other hand, conventional warfare maneuvers can be seen on television channels or social media networks.

There is no doubt that the war in Ukraine is being fought on two levels for cyber issues expert Regine Grienberger from the German Ministry of Foreign Affairs. Grienberger distinguishes between two types of combatants: conventional troops on the battlefield and invisible virtual warriors - "cyber mercenaries," who operate from completely different states and continue to participate in combat operations conditioned by the overload of information systems, by massively accessing certain websites. The result is the cessation, very slow functioning, or even total blocking of networks. This is a popular method both in the civilian and military sectors[26].

Although cyber threats are not unprecedented, says cybersecurity expert Benoît Grunemwald, in the context of the Russo-Ukrainian war, we are witnessing an intensification of cyber attacks from Russia on Ukraine. The war between Russia and Ukraine can be characterized not only as a war fought on the ground through the use of force but also as an active war conducted in cyberspace. There are no planes or tanks here, but computers and the internet are the only weapons. For Michel Baud, "the war in Ukraine, especially in cyberspace, represents a well-coordinated operation carried out by a group of citizens through information and communication systems"[27].

The cyber war, as part of the Russian Federation's military aggression in Ukraine, has been significant, marking the largest conflict in the cyber era. The cyber operations have been extensive, involving phishing, DDoS attacks, and propaganda. Russia has been a key player, engaging in numerous cyber

[26] M. Fürstenau, *Ucrania: tropas convencionales y guerreros virtuales*, <https://www.dw.com/es/guerra-en-ucrania-tropas-convencionales-y-cibercombatientes-invisibles/a-65403959> (12.09.2024).

[27] C. Dugoin-Clément, *Ukraine, crises, conflicts, droit international et cyberspace*, chrome-<extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.defnat.com/pdf/Dugoin-Clement%20(T%201542)_0ML8HxA2l.pdf> (12.09.2024).

operations against Ukraine. Thus, the cyber attacks are part of Russia's strategy to wage an informational war, used alongside conventional military tactics[28]. A number of hackers aligned with the Russian government have carried out hundreds of cyber attacks against Ukraine since Moscow invaded the neighboring country, said the American giant Microsoft in a report. Microsoft emphasized that in Russia's "hybrid" warfare tactics, these cyber attacks are often combined with military actions on the battlefield. "Even before the invasion, we saw at least six national actors aligned with Russia launching over 237 operations against Ukraine," detailed Microsoft, which works with Ukrainian cybersecurity experts and private companies to counter such attacks. The company claimed that this cyber war has included "destructive attacks that are ongoing and threaten civilian welfare." It also stated that it has detected nearly 40 destructive cyber attacks, targeting hundreds of systems, with one-third directly targeting Ukrainian government organizations at all levels (national and local), while another 40% targeted the country's critical infrastructure. "These actors often modify their malware with each action taken to avoid detection," the report mentioned. According to statements presented in the report, cyber attackers began preparing the campaign in March 2021, nearly a year before Vladimir Putin ordered Russian troops to invade Ukraine[29].

According to information published by UATV citing the Security Service of Ukraine, Russia carries out an average of over ten cyber attacks per day on the neighboring country. Throughout the year 2022, the SBU stopped over 4,500 cyber attacks directed towards Ukraine. Furthermore, even before the war between the two states began, Ukraine had repelled numerous massive attacks. As expected, since the beginning of the Russo-Ukrainian war, the number of attacks has significantly increased. To get a comprehensive picture of the situation regarding Russia's cyber attacks on Ukraine, it is necessary to compare the launched attacks. Thus, in 2020, around 800 cyber attacks were launched against Ukraine. By 2021, this number had increased to 1,400, and in 2022, it reached over 4,000 cyber attacks. From this, we see how the Russian Federation resorts to the use of special cyber operations to target energy, logistics, and military installations, as well as the computing centers of Ukrainian state organizations—a significant detail, as it differentiates modern

[28] C. Soare, *Invazia rusă în Ucraina, devine şi primul război cibernetic din istorie: Kievul susține că Rusia se folosește de cooperarea cu China pentru a efectua atacuri cibernetice*, <https://www.defenseromania.ro/invazia-rusa-in-ucraina-in-primul-razboi-cibernetic-din-istorie-kievul-sustine-ca-rusia-se-foloseste-de-cooperarea-cu-china-pentru-a-efectua-atacuri-cibernetice_626906.html#google_vignette> (12.09.2024).

[29] *Guerre en Ukraine: Pourquoi.., op. cit.*

wars from wars of the past. It is about depriving the other party of obtaining resources, in fact. Additionally, it is a wise move to attack databases[30].

Ukraine is often described as a playground for Russian hackers, who have conducted attacks to test techniques and tools. In 2015, Ukraine's power grid was disrupted by a cyber attack called Black Energy, which caused a short-term outage for around 80,000 customers of a utility company in western Ukraine. A year later, another cyber attack known as Industroyer left nearly a fifth of Kiev's population without electricity for about an hour[31].

With the onset of the ground invasion, a wave of cyber attacks on critical infrastructure in Ukraine such as nuclear or electrical power plants, water purification and treatment plants, gas distribution centers, communication antennas and towers, railways, etc., was expected. However, in a scenario of ground war conflict, most of these attacks were carried out through physical bombardments rather than the sophisticated cyber attacks that had been planned. These operations were reported by various Russian media sources, as well as by the creation of specific platforms and accounts on social networks for this purpose[32].

In many cases, third parties were paid for their maintenance and management. Indeed, one of the conclusions that can be drawn from what was observed in the war in Ukraine is that Russia, in addition to military forces, resorts to the use of cyber forces that have not always been its own. In many cases, the Russian government funded cybercriminals and mafias to carry out various operations as mercenaries, leveraging the knowledge they had from their traditional activities before the war. This is the case with various ransomware mafias or botnet owners. There were even groups that supported these campaigns for ideological reasons, without the need for significant economic incentives. These types of attacks usually attempt to collect sensitive information about troop movements, military strategy, supply of essential goods and weapons, etc. In practice, in all cases, there were spear-phishing attacks, meaning illegitimate emails carefully crafted so as not to raise suspicions among their victims and to be perceived as legitimate and trustworthy. When these attacks were successful, the access credentials of the victims were compromised, allowing adversaries to access critical resources, almost always data. This data was not always related to the collection of military information; sometimes, it was used in default campaigns both in Ukraine and in other allied countries. Hack-and-leak operations usually leak

[30] *Así es la guerra cibernética que están librando Rusia y Ucrania. Las trincheras digitales en 2022,* <https://cincodias.elpais.com/cincodias/2022/12/27/lifestyle/1672132222_772838.html#> (12.09.2024).

[31] J. Tidy, *Rusia y Ucrania: los 3 ciberataques rusos que más teme Occidente*, <https://www.bbc.com/mundo/noticias-60850173> (12.09.2024).

[32] *Ibidem.*

information about the victims of Ukrainian combatants, the hesitancy of various governments when it comes to sending weapons to Ukraine, internal discussions about military strategy or peace negotiations, etc. In addition to the aforementioned attacks, others have been observed, which deserve attention due to their novelty or sophistication, almost all related to telecommunications infrastructures. The first was the attack on Viasat an hour before the invasion began. This is an American company in which the Ukrainian army trusted to provide satellite communications links[33].

The Russian military used malware called AcidRain to completely disable thousands of communication terminals in the KA-SAT network, including routers and modems. This attack also affected other European infrastructures, such as wind power generation turbines. The second attack repeated in recent months was based on hijacking Border Gateway Protocol (BGP) sessions. These types of attacks allow the manipulation of routing protocols on which the Internet relies, so that routers can select the worst-intentioned paths for network traffic passing through attacker-controlled devices.

Some experts predicted an escalation in 2023 of cyber attacks carried out by Russia, both in terms of number and scope, as well as potential victims. These attacks have been a powerful tool to reach areas of Ukraine further away from regions subject to traditional warfare, while Russian forces were bogged down in the Eastern part of the country[34]. Pro-Moscow hackers "used destructive programs to disrupt and degrade Ukraine's military and government capabilities," including attacking civilian infrastructure to undermine Ukrainians' confidence in national capabilities[35].

Since the beginning of the war, Russia has implemented at least nine families of Wiper malware and two types of ransomware against over 100 Ukrainian government and private organizations[36]. Strong public-private cyber defense arrangements, as well as Ukrainian preparedness and resilience, have

[33] *Ibidem*.

[34] M. Beltrán, *El papel del ciberconflicto en Ucrania sigue siendo una incógnita un año después*, <https://www.eleconomista.com.mx/tecnologia/El-papel-del-ciberconflicto-en-Ucrania-sigue-siendo-una-incognita-un-anodespues-20230506-0028.html> (12.09.2024).

[35] *Los ciberataques rusos aumentaron un 300% en 2022 en países de la OTAN*, <https://www.france24.com/es/minuto-a-minuto/20230216-los-ciberataques-rusos-aumentaron-un-300-en-2022-en-pa%C3%ADses-de-la-otan> (12.09.2024).

[36] M. G. Pascual, *Por qué Rusia no ha logrado ganar la guerra cibernética en Ucrania*, <https://elpais.com/tecnologia/2023-02-14/por-que-rusia-no-ha-logrado-ganar-la-guerra-cibernetica-en-ucrania.html> (12.09.2024).

successfully defended against most of these attacks, but Russia's activity continues[37].

According to statements made in London by Viktor Zhora, a member of the leadership of the State Special Communications and Information Protection Service of Ukraine, "cyber attacks on Ukraine's infrastructure have tripled during the war months and have often been destructive"[38]. The impact of cyber attacks on Ukraine from Russian actors is presented in the report of the Ukrainian SSSCIP service. Thus, according to the report, there is evidence demonstrating that Russia is waging a war that fits the pattern of hybrid warfare. SSSCIP gives the example of Russian attacks on the energy sector, which are said to have been a significant target of Russian hackers since the beginning of the invasion. Furthermore, the report shows that cyber attacks and those on the media sector usually precede conventional attacks. The SSSCIP study shows that Russia's conventional attacks are often preceded by cyber attacks, which is why the war in Ukraine also falls within the parameters of cyber warfare. Although Russia has repeatedly denied that hacker attacks are orchestrated by the Kremlin, according to SSSCIP, cyber attacks on Ukraine have tripled since the beginning of the war.

In this context, attention should also be paid to the analysis elaborated by specialists from Check Point Research, according to which, cyber attacks in the first days of the Russian invasion and the number of cyber attacks on Ukrainian government infrastructure increased by 196%, while attacks on the Ukrainian commercial sector increased by 4%. Furthermore, according to research conducted by experts from Check Point Research, cyber attacks against Ukraine began in 2014, following the illegal annexation of Crimea, intensifying from February 2022 onwards, affecting the distribution chains of medicines, food, and war supplies most severely[39].

The attacks have taken various forms, but among the tactics used most frequently are deepfakes, phishing emails, malware attacks, Distributed Denial of Service (DDoS) attacks, and information theft. According to SSSCIP, cyber attacks on Ukraine have tripled since the beginning of the war. However, cyber warfare traces its roots back to 2014, the year of Russia's annexation of Crimea. In March 2014, when Russia began its strategy to annex the territory, a DDoS attack hit Crimea's communication systems. Although cyber attacks often precede conventional attacks, sometimes they occur in tandem. One month

---

[37] *¿Se está reagrupando Rusia para una nueva ciberguerra*?, https://news.microsoft.com/es-es/2023/03/17/se-esta-reagrupando-rusia-para-una-nueva-ciberguerra/> (12.09.2024).

[38] D. Temple-Raston, *In recent interview, ousted Ukrainian cyber official spoke about new Russian attacks, long-term plans*, <https://therecord.media/victor-zhora-interview-click-here-ousted> (12.09.2024).

[39] *2023 Cyber Security Report*, <ttps://www.mvrop.org/cms/lib/CA01922720/Centricity/Domain/59/2023-cyber-security-report.pdf> (12.09.2024).

before the invasion of Ukraine, hackers displayed the message "expect the worst" on 70 official government websites[40]. In May 2022, DDoS attacks continue against Ukraine. They target the city council of Odessa, a cyber attack followed by a conventional one on the residential infrastructure of the city. Thus, Russia's strategy is to show doubt among the Ukrainian population about the government's ability to manage the country's infrastructure. SSSCIP states that "cyber attacks are designed to escalate the chaos of conventional invasion, to disrupt the administration of the country, and to cause major damage to infrastructure"[41].

According to the State Special Communications and Information Protection Service of Ukraine, cyber aggression is an offensive tactic of Russia. This takes the form of cyber attacks on communication services and institutions of the country[42]. In this context, several Ukrainian state agencies, including the state energy company, reported cyber attacks or technical disruptions on January 24, 2024, affecting their IT systems and their ability to communicate with the public. Naftogaz, Ukraine's largest oil and gas company, stated that a "large-scale cyber attack" on one of its data centers took its website and call centers offline. Additionally, within the context of cyber attacks conducted by the Russian Federation against Ukraine, there is also the piracy on January 21, 2024, targeting a Ukrainian bank: The largest mobile-only bank in Ukraine was targeted by hackers. Thus, Monobank was targeted with 580 million service requests in a single attack. It is worth noting the cyber attacks against Ukrainians on the eve of the NATO Summit on July 11-12 in Vilnius, Lithuania. BlackBerry researchers have determined that the threat actor was RomCom, who targeted Ukraine supporters scheduled to attend the conference[43].

In this context, Microsoft has issued warnings about a credential theft campaign backed by Russia. Microsoft's security team stated that evidence of cyber attacks orchestrated by the state-backed group Midnight Blizzard, also known as Nobelium, has been found, targeting personal credentials. Midnight Blizzard hackers use residential proxy services to obfuscate the source IP address of their attacks, which typically target governments, IT service providers, NGOs, the defense industry, and critical manufacturing. Additionally, Nobelium is believed to be behind attacks on Ukrainian military

---

[40] I. Breilean, *Războiul cibernetic. Istoria atacurilor ruseşti şi mărturia unui voluntar din „Armata IT" a Ucrainei*, <https://romania.europalibera.org/a/razboi-cibernetic-aramata-it-ucraina/32235520.html> (12.09.2024).

[41] *Ibidem*.

[42] *Ibidem*.

[43] J. Masters, *Russia-Ukraine War: Cyberattack – Kinetic Warfare Timeline*, <https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion> (12.09.2024).

targets, countries providing military assistance to Ukraine, and other organizations opposing Russia[44].

A wave of cyber attacks targeting Ukrainian government agencies and information technology vendors occurred on June 15, 2023, by a group called "Cadet Blizzard," which has been active since 2020. Furthermore, in the context of analyzing Russia's cyber attacks on Ukraine, the activity of the 16th Unit (known as Turla, an elite Russian espionage group) of the Russian Federal Security Service, or FSB, is noteworthy. They used versions of the Snake malware program to create a peer-to-peer network of hundreds of infected computers to remove material belonging to US allies in North America. The pro-Russian hacktivist group Killnet, a cyber crew posing as "hacktivists" actively targeting opponents of the Russian invasion of Ukraine, is also notable. The responsible for widespread denial of service (DDoS) attacks in Europe and the US, at the end of April, they reorganize as a "private military hacking company." Similarly, Russia's activity in launching malware campaigns against Ukraine includes the Iridium campaign (alias Sandworm). It is believed that Iridium is associated with Russia's military intelligence agency (GRU) and prepares operations in a similar manner to the deployment of malware Foxblade and Caddywiper in the early days of the war[45].

Analyzing the cyber attacks carried out by Russia, they can be divided into three categories[46]:

1. Trust Attacks. Trust attacks refer to cyber attacks that undermine public trust in the government's ability to protect its citizens and provide essential services. In the first week of March 2022, it is believed that some Russian cyber actors were involve in launching DDoS attacks (cyber attacks where website servers are flooded with traffic until they become unstable) against the website of the Ministry of Defense of Ukraine. Similarly, the Russian cyber actor FancyBear was found responsible for engaging in a phishing campaign against a Ukrainian media company, UkrNet.
2. Capability-based Attacks. The capability-based attacks are cyber attacks where the adversary's power is undermined by exploiting cyber weapons to gain access to the adversary's critical infrastructure and disrupt its capabilities. In this context, actions taken by several attackers, believed to be of Russian nationality, during the invasion of

[44] *Ibidem*.

[45] J. Masters, *Russia-Ukraine War: Cyberattack – Kinetic Warfare Timeline*, <https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion> (12.09.2024)

[46] *Dimensiunea cibernetică a conflictului Rusia – Ucraina - Deslușirea primei etape*, <https://dnsc.ro/citeste/dimensiunea-cibernetica-conflictului-rusia-ucraina-deslusirea-primei-etape> (12.09.2024).

Ukraine on February 24, 2022, by Russia, serve as examples. As a result, these actions resulted in the destruction of tens of thousands of satellite internet modems in Ukraine and Eastern Europe. These actions are considered to be among the largest cyber attacks in a war, causing massive disruption to communications at the onset of the conflict. In the initial phase of the war, the prominent Russian cyber actor Sandworm was largely absent for unknown reasons. However, the group made its presence felt in the second phase when it was revealed that they attempted to cause a power outage through malware that could have affected two million people.

3. Control-based Attacks. The control-based attacks refer to physical attacks on cyber infrastructures, where the main goal is to gain control over the adversary's critical infrastructure. From this perspective, two notable cyber attacks stand out: 1) on March 1, 2022, a projectile strike on television towers in Kiev coincided with a cyber attack on media companies, and 2) a few days later, during the occupation of the Europe-Zaporizhzhia nuclear power plant, a Russian cyber actor was detected in the networks of a Ukrainian nuclear energy company.

The attackers supported by the Russian government have engaged in an aggressive effort on multiple fronts to gain a decisive advantage in the cyber warfare space, often with mixed results. This includes a significant shift in the focus of various groups towards Ukraine, a dramatic increase in the use of destructive attacks against the Ukrainian government, military and civilian infrastructure, a rise in spear-phishing activity targeting NATO countries, and an increase in cyber operations. For example, it has been observed that threat actors breach sensitive information to promote a specific narrative. Russian government-supported attackers intensified cyber operations starting in 2021, in the lead-up to the invasion. In 2022, Russia increased targeting of users in Ukraine by 250% compared to 2020. In 2022, attackers supported by the Russian government targeted users in Ukraine more than any other country. While we see these attackers heavily focused on the Ukrainian government and military entities, the campaigns we have disrupted also show a strong emphasis on critical infrastructure, utilities, and public services, as well as media and informational space. Many operations have indicated an attempt by the Main Directorate of the General Staff of the Russian Armed Forces (GRU) to balance competing priorities of access, collection, and disruption throughout each stage of activity.

During this period, the public, energy, media, financial, business, and non-profit sectors in Ukraine suffered the most. Starting from February 24, 2022, Russia's cyber attacks on Ukraine undermined the distribution of medicines, food, and aid. Their impact ranged from hindering access to basic services to data theft and disinformation, including through deepfake technology. Other

malicious cyber activities involve phishing emails, distributed denial-of-service attacks, and the use of data-wiping malware, backdoors, surveillance software, and information stealers. The organizations and governments worldwide have not been indifferent to the hybrid risks presented. Initiatives led by the EU, US, and NATO have been undertaken to neutralize cyber threats and protect critical infrastructure. As part of these initiatives, the EU has activated its cyber rapid response teams (a project under the Permanent Structured Cooperation (PESCO) in the field of security and defense policy) to support Ukraine's cyber defense. Non-governmental and private actors have supported Ukraine through various cyber resilience activities. Since the beginning of the invasion, a significant number of counterattacks have been launched by independent hackers, affecting state, security, banking, and media systems in Russia. The European Parliament has called for intensified cyber security assistance to Ukraine and for the full use of the EU's cyber sanctions regimes against individuals, entities, and bodies responsible for or involved in various cyber attacks targeting Ukraine[47].

The Ukraine-and West cooperation in combating cyber threats

Russia has created the greatest threat to peace and stability in Europe since World War II. Since 2014, the driving force behind the development of the Ukrainian cyber space has been the war with Russia. Although authorities have not been able to act effectively in the cyber space since the beginning of the conflict, it has given rise to a cyber ecosystem capable of adapting to the wartime context. This ecosystem has contributed to the defense of the country at all levels, both among citizens and among state and private actors. Although there are still many objectives to be achieved, the invasion of Ukraine has become a catalyst for cyber development, which has become a key player in the Department of Defense. In addition to kinetic warfare, Ukraine currently faces the enemy in both its informational space and in the cyber domain, areas that have often been considered secondary in a high-intensity armed conflict. Cyber sabotage, as well as cyber espionage, are integral parts of the conflict. Taken by surprise by the absence of national cyber security and a clear policy on pollution of the infosphere, Ukrainian authorities have been led to make colossal efforts in the cyber domain[48].

[47] *Russia's war on Ukraine: Timeline of cyber-attacks*, <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549> (12.09.2024).

[48] A. Kryvetska, *Comment l'écosystème cyber ukrainien s'est-il adapté à la guerre?*, <https://www.diploweb.com/Comment-l-ecosysteme-cyber-ukrainien-s-est-il-adapte-a-la-guerre.html> (20.09.2024).

According to statements by Josep Borrell, the High Representative for Foreign Affairs and Security Policy, the Council has made decisions regarding a series of measures to support Ukraine's resilience against Russian aggression. The Council has adopted a decision to provide macro-financial assistance of 1.2 billion euros and has decided to support the professional military training of Ukraine under the European Peace Instrument. Additionally, the EU will enhance its support for combating cyber attacks and disinformation by sending a mission of experts to the country[49].

In order to counter Russian cyber attacks, Ukraine has signed security agreements with its Western allies, hoping to receive additional support in cyber security, military, and humanitarian areas as the ongoing war with Russia reaches the three-year mark. Security agreements for Ukraine are based on the commitment made by the Group of Seven (G7) countries in July 2023. Ukraine has already concluded 10-year agreements with the United Kingdom, Germany, France, and Denmark – the first non-G7 country to finalize the agreement. Additionally, Norway, the Netherlands, and Italy have offered their support to Ukraine for strengthening the defense industry and countering hybrid threats, such as cyber warfare[50].

According to the agreements, Ukraine will receive support in five areas where the war is being waged - on land, in the air, at sea, in space, and in the cyber domain. The cyber support primarily involves assistance to help Ukraine protect its networks from Russian cyber attacks and counter disinformation. For example, the security agreement with Denmark, signed during Danish Prime Minister Mette Frederiksen's visit to Ukraine, promises to assist Ukraine in "preventing, detecting, and countering Russian cyber aggression, cyber espionage, and hybrid warfare". This also includes "strengthening cyber diplomacy, providing technical assistance to Ukraine, and enhancing its cyber resilience". Germany has also committed to helping Ukraine protect its infrastructure from cyber attacks and to modernize the country's security and information architecture, according to the agreement concluded in early February. Berlin will also provide training for Ukrainian experts in cyber security "based on EU standards in IT security".

In this context, the support offered to Ukraine by France is also noteworthy. France will collaborate with Ukraine "to increase the cost of irresponsible use of cyber capabilities by Russia and other hostile state and non-state actors". Paris will also assist Kyiv in combating cybercrime and organized crime[51].

---

[49] *Consiliul Afaceri Externe, 21 februarie 2022*, <https://www.consilium.europa.eu/ro/meetings/fac/2022/02/21/> (20.09.2024).

[50] *Ukraine signs security deals with Western allies to help counter Russian cyberattacks*, <https://therecord.media/ukraine-signs-security-deals-with-western-allies-over-russian-cyberattacks> (20.09.2024).

[51] *Ibidem*.

As the conflict in Ukraine continues, experts have drawn attention to the types of cyber attacks that Russia could conduct against its neighboring country, and thus the international community has mobilized to help the Ukrainian state remotely[52].

As a result of the Joint Declaration of Support for Ukraine jointly issued by the leaders of the Group of Seven (G7) and Ukraine on the margins of the NATO Summit in Vilnius on July 12, 2023 ("G7 Joint Declaration"), the Agreement between Ukraine and Canada was signed on February 24, 2024[53].

Since the large-scale invasion of Ukraine by Russia in February 2022, Canada has provided multidimensional support to Ukraine, including diplomatic, financial, humanitarian, and military assistance, support for development, information, and cyber security, as well as assistance for restoring peace and stability and implementing immigration measures to help Ukrainians settle safely from Russian aggression. Since 2022 and since the beginning of Russia's large-scale invasion of Ukraine, Canada has committed to providing Ukraine with military assistance worth over $2.4 billion. The participants will continue to strengthen their cooperation in defense, building on the strong relationships established between their military and defense institutions since the launch of Operation UNIFIER in 2015, as well as the significant military training and assistance provided by Canada before and after Russia's large-scale invasion.

According to the provisions of Part IV, "Areas of Continued and Enhanced Cooperation and Long-Term Support", Section D, "Cyber Security and Resilience":

1. The states will work together to enable Ukraine to detect, deter, and disrupt Russian cyber aggressions, cyber espionage, and hybrid warfare operations, including maintaining cyber resilience and protecting critical infrastructure against malicious cyber attacks. This objective can be achieved through cooperation and information exchange on cyber threats; implementing joint initiatives; training specialists from defense services, intelligence services, special services, and law enforcement agencies in Ukraine; as well as providing cyber assistance to Ukraine;
2. The participants will work together to detect and deter the irresponsible and malicious use of cyber capabilities by the Russian Federation and other hostile actors, whether state or non-state, against the Participants;

---

[52] *Acord România-Ucraina privind cooperarea în domeniile digitalizării și protecției cibernetice*, <https://www.euractiv.ro/infosociety/acord-romania-ucraina-privind-cooperarea-in-domeniile-digitalizarii-si-protectiei-cibernetice-65107> (20.09.2024).

[53] *Accord de coopération en matière de sécurité entre le Canada et L'Ukraine*, <https://www.international.gc.ca/world-monde/Issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/agreement-ukraine-accord.aspx?lang=fra> (20.09.2024).

3. Recognizing the importance of building strong cyber defense capabilities against state and non-state actors and wishing to expand cooperation in this important area, the participants will:
   - exchange information on national cybersecurity policies, best practices, and lessons learned to strengthen their respective cyber security and resilience;
   - explore new areas of cooperation and new opportunities in the defense and cybersecurity fields;
   - continue to promote exchanges of experts in this field.

Specifically, Canada will continue to:

- provide specific assistance to Ukraine in the field of cyber defense;
- collaborate with partners to coordinate the strengthening of civilian cyber capabilities in Ukraine. This coordination aims to help Ukraine defend against ongoing malicious cyber activities and meet its long-term cyber resilience needs[54].

An important diplomatic step for Ukraine is the signing of a bilateral security agreement by Emmanuel Macron and Volodymyr Zelensky in Paris on February 16, 2024, guaranteeing long-term civil and military support for Ukraine, which has been at war for two years. This ten-year pact follows the commitments made by the G7 at the NATO Summit in Vilnius in July 2023. In addition to the €1.7 billion in 2022 and €2.1 billion in 2023 provided to Ukraine, France commits to providing €3 billion in additional military support to Ukraine in 2024. Paris aims to help Ukraine strengthen its military capabilities to defend its territory and deter future attacks, providing it with equipment and training for Ukrainian forces. As Russia conducts massive disinformation campaigns, signatories to the agreement commit to "combat digital interference and information manipulation" by Moscow, as well as "global propaganda". The agreement provides for "joint education and training programs" for professionals in information integrity[55].

Thus, according to Chapter II, "Cooperation in Security", Section "General Cooperation to Enhance Ukraine's Security", the partnership with France will help Ukraine join collective tools to combat foreign interference and information manipulation, primarily Russian propaganda and disinformation campaigns. Additionally, according to the agreement provisions, states will collaborate to enable Ukraine to detect, deter, and disrupt cyber aggression,

---

[54] *Ibidem*.

[55] *Guerre en Ukraine: aide militaire, assistance en cas d'agression... Ce que contient l'accord de sécurité signé entre Kiev et Paris*, <https://www.francetvinfo.fr/monde/europe/manifestations-en-ukraine/guerre-en-ukraine-aide-militaire-assistance-en-cas-d-agression-ce-que-contient-l-accord-de-securite-signe-entre-kiev-et-paris_6371677.html> (20.09.2024).

cyber espionage, including by enhancing cyber resilience and protecting critical infrastructure against cyber attacks, while also supporting Ukraine's modernization and reform of its security architecture and providing international technical services. The participants will work together to increase the cost of the irresponsible use of cyber capabilities by the Russian Federation and other hostile state and non-state actors against the participants. They will also enhance their operational cooperation in fighting cybercrime and deepen Ukraine's cooperation with EU and NATO structures in cybersecurity[56].

The cyber attacks have increased by 300% between 2020 and 2022 in NATO countries, and by 250% in Ukraine, according to a report by Mandiant, a Google-owned specialized company. Ukraine needs support to "detect, deter, and disrupt any cyber aggression, any cyber espionage". Cooperation in information, counterespionage, fighting serious crime, and organized crime is also planned. This involves combating the infiltration of individuals and groups with criminal influence into Ukrainian society. Signatory countries must cooperate in investigations and joint operations[57].

Equally noteworthy is the signing of the agreement for the development of relations in the field of digitization and cyber security by the Romanian Minister of Research, Innovation, and Digitalization, Bogdan Ivan, and the Ukrainian Deputy Prime Minister for Innovation, Development of Education, Science, and Technology, Mykhailo Fedorov. "Through the signed Agreement, Romania strengthens its position as a regional hub for emerging technologies and cybersecurity. Thus, by signing this agreement, the groundwork is laid for a mechanism through which the European Union will finance concrete technology transfer and knowledge projects to Ukraine, projects in which Romania will lead the partnership"[58]. Additionally, the agreement ensures "the basis for close and concrete collaboration" of institutions with responsibilities regarding IT&C infrastructure, digitization, and cyber security in the two countries.

The main areas of action include:

- increasing the resilience and protection of digital infrastructure in Ukraine and Romania;
- strengthening the level of cyber protection of national networks and infrastructures in Ukraine and Romania;

---

[56] *Accord de coopération en matière de sécurité entre la France et l'Ukraine*, <https://www.elysee.fr/emmanuel-macron/2024/02/16/accord-de-cooperation-en-matiere-de-securite-entre-la-france-et-lukraine> (20.09.2024).

[57] *Guerre en Ukraine: aide militaire.., op. cit*.

[58] S. Cojocaru, *Acord de cooperare româno-ucrainean în domeniul digitalizării şi securităţii cibernetice. Proiectele beneficiază de finanţare UE*, <https://tvrmoldova.md/article/3f68dd806fe63aea/acord-de-cooperare-romano-ucrainean-in-domeniul-digitalizarii-si-securitatii-cibernetice-proiectele-beneficiaza-de-finantare-ue.html> (20.09.2024).

- developing cloud infrastructure for electronic public services;
- exchanging experience in policy formation in the field of electronic communications and emerging technologies[59].

In response to the Russian threat, both private and governmental entities have made unprecedented efforts to support Ukraine's cyber resilience. According to the British publication The Guardian, for the first time since its establishment, the European Union's rapid cyber response team, led by Lithuania, capable of detecting and responding to a variety of threats, has been involved in helping defend Ukraine against cyber attacks. The British publication also mentioned the collaboration between the Romanian state and the private sector to assist the ongoing fight against cyber attacks in the country, specifically the partnership between the National Cyber Security Directorate (DNSC) and Bitdefender, which offered to provide free support and information about potential threats to the Ukrainian state. Additionally, NATO, which has been working with Ukraine for several years to enhance its cyber defense, signed an agreement a few weeks before the invasion aimed at strengthening cyber cooperation with Ukraine. At the same time, in Ukraine, a whole "IT army" of volunteers was gathered in response to the government's request to support cyber defense efforts[60].

The phenomenon we observe today in Ukraine with the creation of a voluntary cyber army ("IT-Army of Ukraine") does not date back to the invasion on February 24, 2022. The genesis of this type of cyber group dates back to the time of the war in Donbass. What do we understand by a "cyber volunteer"? This is an individual who voluntarily participates in defending his country through cyberspace without financial compensation. It can be either an "ordinary" citizen or an experienced hacker. Generally, two categories are observed: autonomous formations that bring together people of all levels on one hand, and on the other hand, groups of hackers responsible for carrying out sophisticated cyber attacks on enemy infrastructure[61].

Conclusions

With the increasing dependency of society on technology and the internet, new forms of threats to the security of not only states but also businesses and individuals worldwide have emerged - cyber attacks, known as cyber warfare.

[59] *Accord România-Ucraina..., op. cit*.
[60] G.-A. Cristescu, *Mobilizare pentru apărarea cibernetică a Ucrainei. România, în atenţia presei internaţionale după anunţul autorităţilor de a colabora cu Bitdefender*, <https://adevarul.ro/stiri-interne/evenimente/mobilizare-pentru-apararea-cibernetica-a-ucrainei-2154479.html> (20.09.2024).
[61] A. Kryvetska, *op. cit.*

The cyber warfare has become a real threat today, and advanced technology is now a powerful tool to attack, sabotage, and disable the information systems of a country. Due to its transnational and anonymous nature, cyber warfare presents unique challenges to the security of states compared to other forms of conflict. Although the boundaries of cyber warfare may be unclear, as in conventional warfare, the primary objective of cyber warfare is to weaken a country by undermining social cohesion, political stability, and the military and industrial capacity of a state.

The cyber warfare is a growing form of conflict that can have serious consequences for society.

Thus, analyzing the cyberattacks carried out by the Russian Federation against Ukraine, Moscow resorts to leveraging the entire spectrum of IO - from state-sponsored mass media to hidden platforms and accounts. It is worth mentioning that they have been present in the cyber space for over a decade, examining the types of attacks that Russian cyber actors launch in Ukraine, since the Russian cyberattacks against Estonia. The military tensions between Russia and Ukraine have clashed in a continuous cyber conflict for about ten years. Kremlin-backed hackers have unleashed the most destructive cyberattacks in history in recent years. However, the danger of escalating conflict in the cyber domain should not be underestimated, as there are no geographical limits to Russian attack attempts.

In the current circumstances, as the Russian Federation decides to the use of cyber attacks as weapons and tactics to pursue its own interests, it is important for the international organizations, governments, businesses, and individuals to strengthen collaboration to mitigate and diminish risks and to protect their own information systems, including safeguarding their own security. Furthermore, the use of cyber attacks by Russia necessitates urgent measures by the world's states to mitigate the impact that cyber attacks can have on national security, as well as international security. Currently, ensuring cyber security must be viewed as an imperative of the time and a critical priority for national defense and the protection of society as a whole.

BIBLIOGRAPHY:

1. *Accord de coopération en matière de sécurité entre le Canada et L'Ukraine*, <https://www.international.gc.ca/world-monde/issues_ development-enjeux_developpement/response_conflict-reponse_ conflits/crisis-crises/agreement-ukraine-accord.aspx?lang=fra>
2. *Accord de coopération en matière de sécurité entre la France et l'Ukraine*,

<https://www.elysee.fr/emmanuel-macron/2024/02/16/ accord-de-cooperation-en-matiere-de-securite-entre-la-france-et-lukraine>
3. *Acord România-Ucraina privind cooperarea în domeniile digitalizării și protecției cibernetice*, <https://www.euractiv.ro/infosociety/acord-romania-ucraina-privind-cooperarea-in-domeniile-digitalizarii-si-protectiei-cibernetice-65107>
4. Arman D., *Atacul cibernetic-o nouă formă de agresiune în dreptul internațional*, <https://ibn.idsi.md/sites/default/files/imag_file/28-31_23.pdf>
5. *Así es la guerra cibernética que están librando Rusia y Ucrania. Las trincheras digitales en 2022*, <https://cincodias.elpais.com/cincodias/2022/12/27/lifestyle/1672132222_772838.html#>
6. Balmforth T., *Exclusive: Russian hackers were inside Ukraine telecoms giant for months*, <https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/>
7. Beltrán M., *El papel del ciberconflicto en Ucrania sigue siendo una incógnita un año después*, <https://www.eleconomista.com.mx/tecnologia/El-papel-del-ciberconflicto-en-Ucrania-sigue-siendo-una-incognita-un-anodespues-20230506-0028.html>
8. Blanc-Rolin C., *Conflit Russie-Ukraine: la guerre est aussi cyber*, <https://www.dsih.fr/article/4608/conflit-russie-ukraine-la-guerre-est-aussi-cyber.html>
9. Breilean I., *Războiul cibernetic. Istoria atacurilor ruseşti şi mărturia unui voluntar din „Armata IT" a Ucrainei*, <https://romania.europalibera.org/a/razboi-cibernetic-aramata-it-ucraina/32235520.html>
10. Buxton O., *Ciberguerra: tipos, ejemplos y cómo protegerse*, <https://www.avast.com/es-es/c-cyber-warfare>
11. Cojocaru S., *Acord de cooperare româno-ucrainean în domeniul digitalizării şi securităţii cibernetice. Proiectele beneficiază de finanţare UE*, <https://tvrmoldova.md/article/3f68dd806fe63aea/acord-de-cooperare-romano-ucrainean-in-domeniul-digitalizarii-si-securitatii-cibernetice-proiectele-beneficiaza-de-finantare-ue.html>
12. Consiliul Afaceri Externe, 21 februarie 2022, <https://www.consilium.europa.eu/ro/meetings/fac/2022/02/21/>
13. *Cyber warfare: ¿Qué es la guerra cibernética?*, <https://www.metacompliance.com/es/cyber-security-terminology/cyber-warfare>
14. De Santos J. C., *Ucrania | La realidad ha dejado a la guerra cibernética en un segundo plano*, <https://es.euronews.com/2023/02/22/

ucrania-la-realidad-ha-dejado-a-la-guerra-cibernetica-en-un-segundo-plano>
15. *Dimensiunea cibernetică a conflictului Rusia – Ucraina - Deslușirea primei etape*, <https://dnsc.ro/citeste/dimensiunea-cibernetica-conflictului-rusia-ucraina-deslusirea-primei-etape>
16. Dugoin-Clément C., *Ukraine, crises, conflicts, droit international et cyberespace*, <https://www.defnat.com/pdf/Dugoin-Clement%20(T%201542)_0ML8HxA2l.pdf>
17. Fürstenau M., *Ucrania: tropas convencionales y guerreros virtuales*, <https://www.dw.com/es/guerra-en-ucrania-tropas-convencionales-y-cibercombatientes-invisibles/a-65403959>
18. Gavrila A., *La gran ciberguerra de Ucrania que no ocurrió*, <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO99_2022_ADAGAV_Ucrania.pdf>
19. Guedes R., *Guerra Cibernética: Tipos, Armas, Objetivos y Ejemplos de Guerra Tecnológica*, <https://ciberprisma.org/2023/05/10/guerra-cibernetica-tipos-armas-objetivos-y-ejemplos-de-guerra-tecnologica/>
20. *Guerre en Ukraine: aide militaire, assistance en cas d'agression ... Ce que contient l'accord de sécurité signé entre Kiev et Paris*, <https://www.francetvinfo.fr/monde/europe/manifestations-en-ukraine/guerre-en-ukraine-aide-militaire-assistance-en-cas-d-agression-ce-que-contient-l-accord-de-securite-signe-entre-kiev-et-paris_6371677.html>
21. *Guerre en Ukraine: Pourquoi parle-t-on d'une cyberguerre?*, <https://guardia.school/le-lab/guerre-en-ukraine-pourquoi-parle-t-on-dune-cyberguerre.html>
22. *Guerre Russie/Ukraine, une cyber guerre déclarée ?*, <https://tehtris.com/fr/blog/guerre-ukraine-russie-une-cyber-guerre-declaree/>
23. Kryvetska A., *Comment l'écosystème cyber ukrainien s'est-il adapté à la guerre?*, <https://www.diploweb.com/Comment-l-ecosysteme-cyber-ukrainien-s-est-il-adapte-a-la-guerre.html>
24. Libicki M. C., *Cyberwar as a Confidence Game*, <https://www.jstor.org/stable/26270514?seq=8>
25. *Los ciberataques rusos aumentaron un 300% en 2022 en países de la OTAN*, <https://www.france24.com/es/minuto-a-minuto/20230216-los-ciberataques-rusos-aumentaron-un-300-en-2022-en-pa%C3%ADses-de-la-otan>
26. Mackay J., *Cyber warfare: ¿Qué es la guerra cibernética?*, <https://www.metacompliance.com/es/blog/security-awareness-training/what-is-cyber-warfare>
27. Masters J., *Russia-Ukraine War: Cyberattack – Kinetic Warfare Timeline*,

<https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion>
28. Pascual M. G., *Por qué Rusia no ha logrado ganar la guerra cibernética en Ucrania*, <https://elpais.com/tecnologia/2023-02-14/por-que-rusia-no-ha-logrado-ganar-la-guerra-cibernetica-en-ucrania.html>
29. *¿Qué es un ataque cibernético?*, <https://www.ibm.com/mx-es/topics/cyber-attack>
30. *Rusia coordina ciberataques en Ucrania, según Microsoft*, <https://www.dw.com/es/rusia-coordina-ataques-cibern%C3%A9ticos-y-militares-en-ucrania-seg%C3%BAn-microsoft/a-61615216>
31. *Russia's war on Ukraine: Timeline of cyber-attacks*, <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)73354>
32. *¿Se está reagrupando Rusia para una nueva ciberguerra?*, <https://news.microsoft.com/es-es/2023/03/17/se-esta-reagrupando-rusia-para-una-nueva-ciberguerra/>
33. Soare C., *Invazia rusă în Ucraina, devine şi primul război cibernetic din istorie: Kievul susține că Rusia se folosește de cooperarea cu China pentru a efectua atacuri cibernetice*, <https://www.defenseromania.ro/invazia-rusa-in-ucraina-in-primul-razboi-cibernetic-din-istorie-kievul-sustine-ca-rusia-se-foloseste-de-cooperarea-cu-china-pentru-a-efectua-atacuri-cibernetice_626906.html#google_vignette>
34. Temple-Raston D., *In recent interview, ousted Ukrainian cyber official spoke about new Russian attacks, long-term plans*, <https://therecord.media/victor-zhora-interview-click-here-ousted>
35. Tidy J., *Rusia y Ucrania: los 3 ciberataques rusos que más teme Occidente*, <https://www.bbc.com/mundo/noticias-60850173>
36. Trifunović D., Bjelica Z., *Cyber war – trends and technologies*, <https://www.researchgate.net/publication/349942064_Cyber_War_-_Trends_and_Technologies>
37. *2023 Cyber Security Report*, <https://www.mvrop.org/cms/lib/CA01922720/Centricity/Domain/59/2023-cyber-security-report.pdf>
38. *Ukraine signs security deals with Western allies to help counter Russian cyberattacks*, <https://therecord.media/ukraine-signs-security-deals-with-western-allies-over-russian-cyberattacks>
39. <https://www.cisco.com/c/dam/global/es_mx/products/pdfs/58-60-bridge.pdf>
40. *5 amenințări asupra securității cibernetice a statelor europene în contextul războiului ruso-ucrainean*, <https://bit-sentinel.com/ro/5-amenintari-asupra-securitatii-cibernetice-a-statelor-europene-in-contextul-razboiului-ruso-ucrainean/>

„Ante Portas – Security Studies”
2024, No 21
DOI: 10.33674/1202424

Carsten Sander CHRISTENSEN[1]
Denmark

END OF THE CONFLICT IN THE RUSSO-UKRAINIAN WAR (2014-2025) AND ITS CONSEQUENCES AND SCENARIOS

Abstract: *After the end of the Cold War, Ukraine has long played an important, and sometimes overlooked role in the global security order. The still ongoing Russo-Ukrainian war actually began in February 2014. Following Ukraine's Revolution of Dignity, Russia annexed Crimea (27,000 km^2) from Ukraine and supported pro-Russian separatists in the Donetsk and Luhansk regions (around 50,000 km^2) – in the so-called Donbas War. In the years 2014-2022, there were occasional military skirmishes in both of the last-mentioned regions, which also included naval incidents and cyberwarfare. On February 24, 2022, Russia launched a so-called full-scale invasion also named a special military operation on Ukrainian area. In the last two years, several hundred thousands of civilians and soldiers on both sides are dead. Thereby it is the biggest military conflict in Europe in the last eighty years - with the most severe refugee crisis, in recent times. In 2025, Ukraine is on the front lines of a renewed great-power rivalry that many experts say will dominate international relations in the decades ahead. After Donald Trump (R) was elected US-President, on November 5 2024; a historic turning point of European security could be in sight. In this article, however, we will analyze the consequences and the scenarios of an end of the Russo-Ukrainian war. And on what conditions and outcomes a possible peace will be concluded?*

Keywords: *Ukraine, Vladimir Putin, Russia, Volodymyr Zelenskyy, Crimea, Donald Trump, Donbas, China, Black Sea, Zaporizjzja, USA, North Korea*

Introduction

After almost three years of a full-scale war and eight years war-like conditions in parts of eastern Ukraine, in the war between Russia and Ukraine,

[1] Carsten Sander Christensen, PhD, email: arroyoinfancia74@gmail.com

there are four outcomes: Russian victory, Ukrainian victory, Frozen war/long war and enforced peace. Regardless of which scenario emerges, the Ukrainian-Russian region will be will be set back 15-20 years in development compared to the regions surrounding the two countries and especially in comparison with some of the world's largest growth areas China and India. Traumatic sociological, economic and impacts of this war will be inescapable for one of the most important areas in the Euro-Asian region. But in a worse and larger context, the so-called balance of power will be affected in a negative direction for the West, since the Russian-Ukrainian war is a war in the Western Hemisphere area. Vladimir Putin's tactic of acting within the auspices of the BRICS countries can be considered a springboard to return to the Western Hemisphere. Among other things, Putin threatened to pull Russia into the Asian Football Confederation. But it didn't come to anything anyway.

Around 145 million Russians live inside the Russian area, Some of the world's largest reserves of natural deposits of fossil fuels, minerals and other important resources for future development are found in Russia, not least because of the huge country's strategic importance in Euro-Asia. A rule of thumb is that the nation that rule the vast Euro-Asian hinterland, will be one of the most important players in the political and economic development in the area. And if the Russians are thrown into the arms of the Asian part of the area, China will quickly become one of main players. A little like the Chinese presence in the Arctic area, where China has no land[2]. The presence of North Korean troops is also an evidence of that fact[3].

However, regardless of which of the abovementioned four scenarios emerge, the far-reaching and traumatic sociological, economic and political impacts of the war, especially in the Ukrainian/Russian, will be inescapable. Other problems could get even worse for Ukraine, when martial law in a future Ukraine is lifted, the big question is whether the country will be able to maintain sufficient unity and resolve to strengthen its institutions and economy to allow it to recover and defend against a future Russian attack. Furthermore, new scenarios will emerge on the domestic political level. Whether Volodymyr Zelensky will win a election is a little doubtful (Winston Churchill also lost his election after WW2), and new political players, including other Ukrainian military veterans and representatives of parliamentary and presidential elections

[2] S. Bradley, *Ukraine War: Who's winning?*, "The Week UK", November 27, 2024, https://theweek.com/news/world-news/europe/961821/who-is-winning-the-war-in-ukraine (20.12.2024).

[3] S. Kullab, *Thousands of North Korean troops in Russia. What does that mean for the war with Ukraine?*, "AP News", October 31, 2024, <https://apnews.com/article/russia-ukraine-north-korea-war-735ab717dcf92a718adcb68bfbddc653> (20.12.2024).

that are required by Ukraine's constitution. In other words, the country could experience political instability[4].

Four scenarios in general

The ongoing conflict between Russia and Ukraine has had devastating consequences for both nations and the wider world. Rooted in historical tensions, geopolitical interests, and cultural divisions, the war has reshaped the global order and caused immense human suffering. While predicting the exact trajectory of this conflict is challenging, several potential pathways could lead to its resolution. This article explores key scenarios and strategies that could bring about an end to the war, focusing on diplomacy, military outcomes, internal political changes, and the role of the international community[5].

Diplomatic Negotiations and Peace Agreements

One of the most plausible ways to end the conflict is through diplomatic negotiations resulting in a comprehensive peace agreement. This would require both sides to engage in meaningful dialogue mediated by international actors such as the United Nations, the European Union, or neutral countries like Turkey or Switzerland. Key elements of such negotiations could include[6]:

- Territorial Compromises: Discussions about the status of contested regions like Crimea and the Donbas.
- Security Guarantees: Agreements ensuring Ukraine's sovereignty and territorial integrity while addressing Russia's security concerns, such as NATO expansion.
- Economic Reparations: Compensation for war damages and rebuilding efforts in Ukraine.
- Demilitarization Zones: The establishment of buffer zones to prevent future escalations.

While diplomacy offers a peaceful resolution, it is contingent on the willingness of both sides to make concessions – a prospect that remains elusive given the entrenched positions of Russia and Ukraine[7].

---

[4] S. Bradley, *op. cit*.

[5] T. Paffenholz, A. Bramble, P. Poppelreuter, N. Ross, *Negotiating an End to the war in Ukraine: Ideas and Options to Prepare for and Design a negotiation process*, Report 2023, pp. 3-4.

[6] Ch. Stückelberger, *Ukraine-Russia: Twelve Proposals Towards Negotiated Peace*, p. 6, <https://www.fpablovi.org/images/Actualidad/firma/Ukraine-Russia.pdf > (18.08.2024).

[7] I. Ijgyarto, S. Seremet, *After Twenty-Seven Months of War, Ukraine needs Peace*, MKI Report 2024, p. 9, <https://hiia.hu/wp-content/uploads/2024/06/MKI-Report_After-Twenty-Seven-Months-of-War-Ukraine-Needs-Peace.pdf> (20.12.2024).

Military Outcomes

Another scenario involves a decisive military outcome, either through a Ukrainian victory, a Russian victory, or a prolonged stalemate.

- Ukrainian Victory: With continued Western military and economic support, Ukraine could reclaim occupied territories and force Russia to withdraw. This outcome, while possible, would likely require years of sustained conflict and significant resources[8].
- Russian Victory: Conversely, a Russian victory could result from overwhelming military force or internal collapse within Ukraine. However, this outcome seems increasingly unlikely given Russia's logistical challenges and growing international isolation[9].
- Stalemate: A prolonged stalemate, where neither side achieves a decisive victory, could pressure both parties into negotiations. This scenario risks becoming a "frozen conflict" similar to other post-Soviet disputes, such as in Transnistria or Abkhazia.

Internal Political Changes

Political shifts within Russia or Ukraine could dramatically alter the course of the war. In Russia, a change in leadership or public discontent with the war – fueled by economic sanctions and military losses – could lead to a withdrawal or a re-evaluation of its strategy[10].

Conversely, political instability in Ukraine could weaken its ability to resist Russian aggression, potentially forcing concessions.

Economic Pressure and Sanctions

International sanctions have severely impacted Russia's economy, targeting key sectors such as energy, finance, and technology. Over time, these measures could erode Russia’s capacity to sustain the war, incentivizing a negotiated settlement. Simultaneously, continued economic support for Ukraine will be crucial in maintaining its resilience against Russian aggression[11].

---

[8] F. Farrell, *How will the Russia-Ukraine War end? The good, the bad and the ugly scenarios*, “Kyiv Independent”, December 13, 2024, <https://kyivindependent.com/how-will-russia-war-in-ukraine-end/> (20.12.2024).

[9] G. Gressel, *Ukraine’s Survival: Three Scenarios for the war in 2024*, European Council on Foreign Relations, January 31, 2024, <https://ecfr.eu/article/ukraines-survival-three-scenarios-for-the-war-in-2024/> (20.12.2024).

[10] T. Paffenholz, A. Bramble, P. Poppelreuter, N. Ross, *op. cit.*, pp. 39-40.

[11] Ch. Stückelberger, *op. cit.*, p. 6.

Mediation by Third Parties

Neutral or influential third parties could play a pivotal role in mediating an end to the conflict. Countries like China, India, or Turkey, which have maintained relationships with both Russia and the West, could leverage their positions to broker a ceasefire or peace deal. Such mediation would require addressing the core grievances of both sides while ensuring a sustainable and enforceable agreement.

Role of International Institutions

International institutions such as the United Nations, the Organization for Security and Co-operation in Europe (OSCE), and NATO could contribute to conflict resolution by[12]:

- Deploying Peacekeeping Forces: Ensuring compliance with ceasefires and protecting civilians.
- Facilitating Reconstruction: Coordinating global efforts to rebuild war-torn areas.
- Enforcing Accountability: Pursuing justice for war crimes and human rights violations through international courts.

Grassroots and Civil Society Efforts

While often overlooked, grassroots movements and civil society organizations in both countries can foster reconciliation and dialogue. Initiatives promoting cross-border understanding, cultural exchange, and humanitarian aid can lay the groundwork for long-term peace.

Despite these potential pathways, several challenges complicate efforts to end the war:

- Mistrust: Deep-seated mistrust between Russia and Ukraine undermines negotiations.
- Geopolitical Rivalries: The conflict's broader implications for global power dynamics make it difficult to isolate from international politics.
- Domestic Pressures: Both governments face internal pressures to maintain strong positions, limiting their flexibility.
- Humanitarian Crisis: The ongoing suffering of civilians exacerbates tensions and fuels animosities.

---

[12] *President Zelenskyy Peace Formula - Ukraine's Peace Formula Philosophy*, <https://www.president.gov.ua/storage/j-files-storage/01/19/53/32af8d644e6cae41791548fc82ae2d8e_1691483767.pdf> (20.12.2024).

The Russian-Ukrainian war has reshaped the geopolitical landscape, highlighting the fragility of international norms and the devastating consequences of unresolved conflicts. While the road to peace is fraught with challenges, it is not unattainable. A combination of diplomatic efforts, international pressure, and grassroots initiatives could pave the way for a resolution that respects Ukraine's sovereignty, addresses Russia's concerns, and promotes lasting stability in the region. The stakes are high, but so is the potential for a future where peace prevails over conflict[13].

Russian victory

A scenario that is the Russians' ultimate goal. A goal that, according to Vladimir Putin, will be achieved when the Ukrainian provinces of Luhansk, Donetsk, the Crimean peninsula and parts of the Zaporizjzja region are incorporated in the state of Russia. Today Russia controls 20% of the total area of Ukraine. Russian terms of surrender (neutrality, demilitarization, distance to EU and NATO at all levels and a pro-Russian government) and of course recognition of territorial losses, maybe all the Ukrainian coast to the Black Sea, will only be possible, if there is no interference from the West[14]. That means a withdrawal of Western support for Ukraine and furthermore a complete Ukrainian military collapse. But if that happens, it will certainly throw large parts of the Ukrainian population into the arms of the Russians and a high risk of de-centralized insurgencies in the territories annexed by Russia and prolonged instability in the rest of the country. A withdrawal of Western support for Ukraine is, therefore, only theoretical[15].

Theoretically, this could force power into a 'pragmatic' government in Kiev, prepared to accept significant territorial concessions to save Ukraine from further bloodshed and destruction. However, it would create a high risk of decentralized uprisings in the territories annexed by Russia and prolonged instability in the rest of the country[16].

---

[13] *Ibidem*.

[14] M. Episkopos, *What a Russian 'victory' would look like*, Responsible Statecraft - quincyinst.org, May 6, 2024, <https://responsiblestatecraft.org/russia-ukraine-war/> (18.10.2024).

[15] Gressel G., *Ukraine's Survival: Three Scenarios for the war in 2024*, European Council on Foreign Relations, January 31, 2024, <https://ecfr.eu/article/ukraines-survival-three-scenarios-for-the-war-in-2024/> (18.10.2024).

[16] Y. Yakymenko (ed.), *Ukraine from war to peace and recovery*, Razumkov Centre, Kyiv September 2024, p. 5.

Political Perspective

A Russian victory could reshape the geopolitical landscape, particularly in Eastern Europe. Russia might:

- Strengthen its sphere of influence: Successfully annexed territories, such as those in the Donbas region, would solidify Russia's control in Eastern Ukraine. This could establish a precedent for future territorial ambitions and bolster Russia's claims as a dominant regional power[17].
- Undermine Western alliance's: A victory could reveal divisions within NATO and the EU over how to handle Russian aggression, potentially weakening their collective stance against Moscow. This might embolden Russia to challenge other security agreements[18].
- Bolster domestic legitimacy: The Kremlin could use a victory as a propaganda tool to rally national pride and justify the war effort, solidifying President Vladimir Putin's hold on power[19].

Military Perspective

- Demonstration of Russian military prowess: A win would reinforce Russia's image as a capable military force despite setbacks earlier in the war, demonstrating resilience and adaptability[20].
- Strategic gains: Consolidation of territories in Eastern Ukraine would provide strategic depth and valuable resources, including access to critical ports and industries in the region.
- Shift in military doctrine: Lessons learned from the conflict may lead to reforms in Russian military strategies, equipment modernization, and tactics.

Economic Perspective:

- Access to resources: Gaining control over Ukraine's resource-rich regions, such as coal mines, agricultural lands, and natural gas reserves, could enhance Russia's economic self-sufficiency.
- Sanction resilience: If Russia successfully withstands Western sanctions during and after the war, it could signal the emergence of a more

[17] J. Lough, *Four Scenarios for the End of the War in Ukraine*, Chatham House 2024, <https://www.chathamhouse.org/2024/10/four-scenarios-end-war-ukraine> (20.11.2024).
[18] F. Farrell, *op. cit*.
[19] S. Bradley, *op. cit*.
[20] M. Episkopos, *op. cit*.

sanction-proof economy, potentially setting an example for other sanctioned states.
- Reintegration of economic assets: A victory might allow Russia to integrate critical Ukrainian infrastructure, such as ports and energy facilities, boosting its economic capabilities.

Global Impact:

- Challenge to the rules-based order: A Russian victory would mark a significant challenge to the international norms established after World War II, particularly regarding sovereignty and territorial integrity.
- Inspiration for other powers: Other nations with territorial disputes might view Russia's success as a model, potentially destabilizing other regions.
- Shifts in global alliances: Countries aligned with Russia, such as China and Iran, might be emboldened, while Western nations could face difficulties maintaining unified opposition to authoritarian regimes.

Risks and Uncertainties:

Even in victory, Russia might face:
- Long-term insurgencies: Continued resistance from Ukrainians in occupied regions could strain Russian military and economic resources.
- Isolation: A prolonged conflict and territorial gains might cement Russia's pariah status internationally, leading to further diplomatic and economic isolation.
- Economic stagnation: Despite resource gains, long-term sanctions and brain drain could hamper Russia's broader economic prospects[21].

Ukrainian victory

A change in Western policy leading to allies providing the weapons and military support that would enable Ukraine to force the Russian army back to at least the demarcation line by February 23, 2022. A Russian retreat, especially if its hold on Crimea were jeopardized, could have dramatic political consequences within Russia itself, perhaps leading to a period of instability followed by radical reforms and eventual normalization of ties with the West.[22] A longer period of Russian introspection would enable Ukraine to implement deep reforms and accelerate the Europeanization of state institutions, leading to

[21] M. Episkopos, *op. cit.*
[22] G. Gressel, *op. cit*.

a realistic prospect of joining the EU and improving its overall security situation, perhaps with the possibility of rapid integration into NATO[23].

Political Perspective

A Ukrainian victory would have profound implications for both Ukraine and the broader international order:

- Strengthened sovereignty: A victory would reaffirm Ukraine's territorial integrity and sovereignty, sending a powerful message against aggression and imperial ambitions.
- Enhanced national identity: Success on the battlefield could unite Ukrainians further, bolstering national pride and solidarity across political and cultural divides.
- Democratic legitimacy: Ukraine's ability to resist and win could enhance its credibility as a democratic nation, increasing its appeal for EU and NATO membership.

Military Perspective:

- Ukrainian military prominence: A victory would solidify Ukraine's status as a highly capable military force, demonstrating the effectiveness of its leadership, strategy, and adaptability.
- Innovation in warfare: The use of modern tactics, Western technology, and local ingenuity could become a blueprint for asymmetric warfare globally.
- Deterrence for future aggression: Defeating Russia would send a strong deterrent message to potential aggressors, showcasing the consequences of violating international norms.

Economic Perspective:

- Post-war reconstruction: Victory would likely unlock significant international aid for rebuilding infrastructure, reviving industries, and stabilizing the economy, with organizations like the EU, IMF, and World Bank contributing.
- Energy independence: A win could allow Ukraine to secure and develop its energy resources, reducing reliance on Russian supplies and boosting regional energy security[24].

[23] *President Zelenskyy Peace Formula …*, *op. cit*.
[24] Y. Yakymenko, *op. cit.*, pp. 12-13

- Integration with Western markets: Economic reforms tied to victory and reconstruction could fast-track Ukraine's integration into European and global markets[25].

Global Impact:

- Reinforcement of international norms: A Ukrainian victory would bolster the principle of territorial integrity, showing that military aggression cannot succeed.
- Strengthened Western alliance's: Success would validate NATO's and the EU's support, reinforcing the value of collective security and international cooperation.
- Weakened autocracies: Russia's defeat could undermine confidence in authoritarian regimes, while boosting democratic movements worldwide.

Russia's Decline:

A Ukrainian victory could have significant repercussions for Russia:

- Political instability: Defeat might weaken President Vladimir Putin's grip on power, potentially leading to internal political strife or regime change.
- Economic downturn: Losses in the war, compounded by prolonged sanctions, could lead to economic stagnation and diminished global influence.
- Military discreditation: Failure in Ukraine could expose vulnerabilities in Russia's military, damaging its reputation and reducing its ability to project power internationally.

Risks and Challenges:

Even with victory, Ukraine may face challenges:

- Long-term security concerns: Russia might regroup and attempt future aggression, requiring Ukraine to maintain a strong defense posture.
- Economic strain: Reconstruction will be costly and time-intensive, and managing international loans and aid could present governance challenges.
- Social healing: Post-war recovery will involve addressing the psychological and physical toll on citizens, refugees, and displaced communities.

[25] J. Lough, *op. cit*.

Frozen war/long war

A ceasefire that would stabilize the front line and allow both sides to regroup and rebuild their depleted forces in preparation for further fighting. There would be no agreement on Ukraine's future military status or the size of its armed forces. Ukraine would remain formally committed to the goal of full restoration of its 1991 borders.

Political Perspective:

- De facto borders without recognition: A frozen conflict could solidify a status quo where territories under Russian or Ukrainian control remain contested but are not officially recognized internationally. This mirrors past conflicts, such as in Transnistria, Abkhazia, or South Ossetia.
- Challenges to sovereignty: Ukraine would struggle with the loss or contested status of occupied territories, leading to ongoing political tension and incomplete sovereignty.
- Continued Russian influence: A frozen conflict could allow Russia to maintain leverage over Ukraine and disrupt its path toward EU or NATO membership by keeping instability at its borders.

Military Perspective:

- Ceasefire without resolution: A frozen conflict could involve entrenched frontlines with sporadic skirmishes and no active offensives, similar to the Korean Peninsula's situation after the armistice.
- Militarization of borders: Both sides would likely continue heavy militarization along the conflict zones, leading to constant readiness for renewed hostilities.
- Insurgent activity: Ukrainian partisan resistance in occupied territories or potential unrest in contested areas could lead to low-intensity violence, prolonging instability.

Economic Perspective:

- Limited economic recovery: A frozen conflict would hamper Ukraine's full economic revival, as uncertainty over its borders and security would deter foreign investment and economic integration.
- Sanctions stalemate: Western sanctions on Russia would likely persist, while Moscow's counter-sanctions and economic realignments would continue, further entrenching global economic divisions.

- Reconstruction challenges: Ukraine's reconstruction efforts might be constrained by uncertainty in conflict zones, leading to uneven development and prolonged reliance on international aid[26].

Global Impact:

- Geopolitical stalemate: A frozen conflict would reflect the limits of both Western and Russian ambitions, leaving the international community divided over how to proceed diplomatically.
- Prolonged instability: The region would remain a flashpoint, with potential for renewed escalations impacting neighboring countries and international energy and trade routes.
- Normalization of frozen conflicts: The situation could set a precedent for other conflicts where aggressors seek to achieve partial territorial gains without full resolution, undermining international norms.

Social and Humanitarian Perspective:

- Prolonged displacement: Refugees and internally displaced persons (IDPs) might face difficulty returning home, particularly to regions under Russian control or near contested borders.
- Psychological toll: A frozen conflict could perpetuate a sense of uncertainty and trauma for affected populations, hindering long-term reconciliation and rebuilding.
- Divided communities: Families and communities separated by new frontlines might face difficulties reconnecting, leading to generational divides.

Risks and Opportunities:

Risks:

- Unresolved tensions: Without a clear resolution, both sides could perceive the frozen state as temporary, preparing for future escalations.
- Undermined trust in diplomacy: A frozen conflict might signal the failure of international mediation efforts, reducing trust in diplomatic solutions globally.
- Erosion of governance: Prolonged conflict without resolution could weaken state capacity in contested areas.

Opportunities:

[26] J. Lough, *op. cit*.

- Space for diplomacy: A ceasefire could create breathing room for long-term negotiations, confidence-building measures, and eventual conflict resolution.
- Stabilization of daily life: A halt to active fighting could reduce civilian casualties and enable limited economic and social recovery in affected regions.

Long war

A conflict of attrition that allows each side to exhaust the other. Ukraine would continue to fight and try to rebuild at the same time, while incurring ever greater human losses on the battlefield and in migration.

Political Perspective:

- Endurance over resolution: Both Russia and Ukraine might adopt strategies focused on outlasting the other rather than pursuing a decisive victory, entrenching their positions.
- Erosion of political stability: Prolonged conflict could strain leadership in both nations, potentially leading to political instability. In Russia, economic hardships or battlefield losses might weaken Putin's regime. In Ukraine, war fatigue could test public support for the government.
- Normalization of conflict: The war might become a background feature of the geopolitical landscape, with limited international urgency to resolve it as other global crises emerge.

Military Perspective:

- War of attrition: A long war could see both sides suffering significant losses in manpower, equipment, and resources, with incremental gains and losses along entrenched frontlines.
- Evolution of tactics: Both sides would likely adapt their strategies over time, incorporating new technologies, intelligence, and alliances to gain an advantage.
- Mobilization cycles: Sustained conflict could lead to repeated waves of mobilization, affecting civilians and economies as governments struggle to replenish depleted forces.
- Proxy warfare: External actors might increase their involvement, turning Ukraine into a testing ground for new weapons and strategies by NATO countries, Russia, and other global powers.

Economic Perspective:

- Economic stagnation: Prolonged warfare would devastate Ukraine's economy, delaying reconstruction and exacerbating poverty. Russia would also face deepening sanctions, resource strains, and economic isolation.
- Global economic disruptions: Prolonged instability could continue to affect global energy markets, food supplies (Ukraine's grain exports), and trade routes, leading to inflation and economic hardship in other regions.
- War economies: Both nations might shift toward "war economies," where resources are prioritized for military needs over civilian development, entrenching hardship for ordinary citizens.

Social and Humanitarian Perspective:

- Prolonged displacement: Millions of refugees and internally displaced persons (IDPs) could face years without stable homes, creating long-term social and humanitarian crises.
- Generational impact: Children in both countries would grow up in the shadow of war, affecting education, mental health, and future prospects.
- Civilian casualties and destruction: A long war would likely lead to sustained high levels of civilian suffering, with entire towns and cities becoming uninhabitable due to continued shelling and fighting.
- Polarization and hatred: A protracted conflict could deepen animosities between Ukrainians and Russians, making reconciliation and peacebuilding more difficult even after the war ends.

Global Impact:

- Extended geopolitical tensions: NATO and Russia would remain in a prolonged state of confrontation, potentially escalating into direct clashes or further destabilizing other regions, such as the Arctic, the Middle East, or the South Caucasus.
- War fatigue in the West: Over time, Western nations might struggle to maintain unified support for Ukraine, especially if public opinion shifts due to economic pressures or competing priorities.
- Strengthened autocratic alliances: Russia might deepen ties with countries like China, Iran, and North Korea to counter Western sanctions and secure military and economic support, leading to a more polarized global order.

Environmental Perspective:

- Environmental degradation: Prolonged war would cause severe ecological damage, including destroyed farmlands, polluted waterways, and devastated ecosystems, particularly in heavily contested regions.
- Energy infrastructure destruction: Repeated attacks on pipelines, power plants, and other infrastructure could create long-lasting energy shortages and environmental hazards.

Risks and Opportunities:

Risks:

- Escalation beyond Ukraine: A long war increases the risk of the conflict spilling over into other regions, particularly NATO territories or post-Soviet states like Moldova or Georgia.
- Global crisis convergence: A prolonged conflict could exacerbate other global challenges, such as climate change, pandemics, or economic instability, overwhelming international institutions.
- Prolonged suffering: The longer the war continues, the harder it will be to rebuild trust, reconcile, and heal the social fabric of the affected regions.

Opportunities:

- Innovations in defense and resilience: Prolonged war could drive advancements in military technology and civilian resilience, offering future applications for other conflicts or disasters.
- Shift in global alliances: Over time, new alliances and partnerships might emerge as countries reassess their strategic interests in light of the protracted war.

Enforced peace

The elements of this peace must be elements which engage the confidence and satisfy the principles of the American governments, elements in accordance with their political faith and with the practical convictions which the people of America have once for all embraced and undertaken to defend[27]. The terms of the immediate peace agreed upon will determine whether it is a peace for which such a guarantee can be secured. The question on which the future peace and politics of the whole world depend is this: Is the present war a struggle for a just and secure peace, or only for a new balance of power? If it is only a

[27] *Trump urges Putin to avoid escalation in Ukraine war, report says*, France24, November 11, 2024, https://www.france24.com/en/europe/20241111-trump-putin-ukraine (20.11.2024).

struggle for a new balance of power, who will guarantee, who can guarantee the stable equilibrium of the new arrangement?[28]

Political Perspective:

- Transactional diplomacy: True to Trump's negotiation style, an enforced peace would likely focus on striking a deal that prioritizes immediate cessation of hostilities over long-term resolution of underlying issues. He might frame the deal as a win-win compromise, regardless of its durability.
- U.S.-centric framing: Trump could emphasize his role as the "deal-maker" to bolster his domestic and global image, using the peace agreement to showcase U.S. leadership and his personal effectiveness in resolving global conflicts.
- Neutrality on principles: The agreement might sideline complex issues like sovereignty and territorial integrity in favor of pragmatic concessions to both sides, such as autonomy for contested regions or economic incentives.
- Tensions with NATO and allies: A Trump-led peace process could strain relations with NATO and EU allies if they perceive the deal as undermining Ukraine's sovereignty or rewarding Russian aggression.

Military Perspective:

- Ceasefire as a focal point: Trump would likely prioritize a ceasefire to stop active fighting immediately, framing it as a first step toward stability[29].
- Demilitarized zones: The agreement might include the creation of demilitarized zones or peacekeeping forces, possibly involving countries perceived as neutral to both Russia and Ukraine.
- Focus on cost-cutting: Trump's approach could aim to reduce U.S. military aid to Ukraine by emphasizing the need for a "self-sufficient" Ukraine and greater burden-sharing by European allies[30].

Economic Perspective:

- Economic incentives for compliance: Trump could offer or broker economic incentives, such as lifting certain sanctions on Russia or

[28] S. F. Santos, *Trump ally says Ukraine focus must be peace, not territory*, BBC News, November 9, 2024, <https://www.bbc.com/news/articles/czxrwr078v7o> (20.11.2024).
[29] *Ibidem*.
[30] S. F. Santos, *op. cit*.

providing reconstruction aid to Ukraine, tied to adherence to the peace deal.

- Energy diplomacy: The agreement might include provisions related to energy, such as reopening gas pipelines, restoring Ukraine's energy infrastructure, or allowing Russia to maintain certain energy exports under monitored conditions.
- Trade-offs for Western support: Trump might push European nations to finance more of Ukraine's reconstruction and security to lessen the financial burden on the U.S.

Global Impact:

- Reshaped global alliances: Trump's peace initiative could shift global alliances, as countries adjust to his unorthodox approach and its implications. For instance:
- Russia might gain partial legitimacy if the deal includes formal recognition of annexed territories.
- Ukraine could face reduced Western support if the deal appears to compromise its sovereignty.
- China and other global powers might use this scenario to test U.S. resolve in other areas, like Taiwan.
- Potential new precedent: An enforced peace by Trump could set a controversial precedent where aggressors are partially rewarded to secure short-term stability[31].

Social and Humanitarian Perspective:

- Unresolved grievances: A peace deal focused on expedience might fail to address deeper issues like displaced populations, war crimes, or the reintegration of occupied territories, leaving lingering resentment.
- Humanitarian aid as a bargaining chip: Trump might advocate for increased international humanitarian aid as a visible benefit of the peace deal, framing it as a success while leaving long-term reconciliation to local governments.

Risks, Challenges and Opportunities:

[31] Thompson Reuters, *Source says Trump advice Putin not to escalate Ukraine war, Kremlin denies conversation,* CBC.CA, November 11, 2024, <https://www.cbc.ca/news/world/trump-putin-phone-call-ukraine-1.7380033> (20.11.2024).

Risks:

- Undermined international norms: By brokering a deal that compromises on sovereignty or territorial integrity, Trump could weaken global norms against aggression, emboldening other authoritarian regimes.
- Fragile agreement: A deal driven by Trump's emphasis on speed and optics might lack the institutional or multilateral support needed to ensure its durability, risking a relapse into conflict.
- Polarization within Ukraine: Concessions, such as granting autonomy to contested regions or allowing Russian influence to persist, could divide Ukrainian society and weaken its government.

Challenges:

- Securing buy-in: Trump's approach might face skepticism or resistance from both Kyiv and Moscow, particularly if the terms are seen as favoring one side or failing to address key demands.
- Maintaining U.S. credibility: NATO allies and other global actors might question the U.S.'s commitment to Ukraine and international norms, especially if Trump prioritizes a deal over principle.

Opportunities:

- Immediate halt to hostilities: Even if imperfect, an enforced peace could save lives and reduce civilian suffering by stopping active fighting.
- Pathway to long-term negotiations: A ceasefire or interim agreement could create space for more comprehensive peace talks in the future.
- Showcase of U.S. leadership: If successful, Trump could frame the deal as a landmark achievement, potentially improving U.S. influence in other global conflicts[32].

Conclusion

The almost 12-year war-like situation in Ukraine has fundamentally changed the country. And within the last three years, Russian society has also begun to change fundamentally. The region will be marked by the events for many decades, regardless of what form of peace, which of four scenarios will be realized or a continued long war will take effect. In the last three years, an additional dimension has emerged in the violent conflict: a global perspective on a future world community with Western countries on one side and Russia, China, partly India and other BRICS countries on the other. This means that a possible end to the war will have consequences for the entire world and not only Ukraine and Russia.

[32] *Ibidem.*

How could Ukraine’s security be guaranteed?

Ukraine is demanding to be brought into NATO. But neither Donald Trump nor other NATO nations has expressed a desire for it; and Vladimir Putin would do everything in his power to block it. One other possibility is for a demilitarised zone, preserved by peacekeeping troops. It has been reported that Donald Trump would call on EU and British troops to enforce a buffer zone between the Russian and Ukrainian armies. This would be expensive and possibly dangerous for those nations, and Russia might well be implacably opposed. Alternatively, some have proposed the "Israel model": Ukraine remains formally outside NATO but is plentifully supplied with weapons and diplomatic support by the US and the West.

Is peace possible in the near future?

This depends on a series of complex interlocking issues: essentially, the tolerance of both sides for continued fighting, and the extent of Western support. And in a longer perspective of the rest of the world's attitude to the events. The two warring countries did come close to reaching a deal before, in Istanbul, weeks after the war began. It was proposed then that Ukraine would give up its NATO ambitions and commit to neutrality, but would have security guarantees from Western nations. The talks fell apart, for reasons that are disputed, with key issues still undecided. Negotiations under Donald Trump's auspices could be difficult for Ukraine, because the country shall focus on peace and not on territory.

Who will loose first?

Ukraine's weaknesses are clear: it is outmanned and outgunned, and facing a renewed onslaught on its eastern front despite the massive losses it has inflicted on the invading Russians. Its energy grid is pulverised daily. President Volodymyr Zelensky is unwilling to mobilise more troops by lowering the age for military service from 25 to 18, though the US urged him to do so last month. But the pressures on Russia are considerable, too. Casualty figures are hard to verify, but Ukraine estimates that 200,000 Russian soldiers have been killed and 600,000 more wounded (compared to 50,000 Ukrainian dead and 370,000 wounded). Although there is practically no internal opposition to Putin, the war is not popular: independent polling suggests 49% of Russians support withdrawing troops even if it means not achieving stated military goals. Perhaps the most pressing issue, though, is the economy. The official inflation rate has reached 8.5%, even though the central bank has raised its main interest rate to 21%. Prices of staples are going up by more than 20% per year. The

government is expected to raise rates again this month, and is spending its savings.

Will the US government succeed in bringing about rapid peace in the region?

To end the war immediately is possible but may have unintended effects in Ukraine, in Russia and in the rest of the world. The US has spent more than $120bn in aid to Ukraine since the war began in February 2022, making it by some distance the largest donor. However, domestic support for arming Ukraine appears to have waned, particularly among Republicans, and isolationism is prevalent in the Maga movement. The war in Ukraine is by no means a top topic in the United States or Canada for that matter. Domestic political issues may become so serious that the war in Ukraine must be put on hold by the American administration and the president. After the election, Donald Trump Jr reposted a meme warning President Volodymyr Zelenskyy: "You're 38 days from losing your allowance". Trump's own position, though, has been fluid. He has presented no plan, and has not said how he would bridge the gap between apparently irreconcilable Russian and Ukrainian positions.

BIBLIOGRAPHY:

1. Bradley S., *Ukraine War: Who's winning?*, The Week UK, November 27, 2024, <https://theweek.com/news/world-news/europe/961821/who-is-winning-the-war-in-ukraine>
2. Episkopos M., *What a Russian 'victory' would look like*, Responsible Statecraft - quincyinst.org, May 6, 2024, <https://responsiblestatecraft.org/russia-ukraine-war/>
3. Farrell F., *How will the Russia-Ukraine War end? The good, the bad and the ugly scenarios*, "Kyiv Independent", December 13, 2024, <https://kyivindependent.com/how-will-russia-war-in-ukraine-end/>
4. Gressel G., *Ukraine's Survival: Three Scenarios for the war in 2024*, European Council on Foreign Relations, January 31, 2024, <https://ecfr.eu/article/ukraines-survival-three-scenarios-for-the-war-in-2024/>
5. Ijgyarto I., Seremet S., *After Twenty-Seven Months of War, Ukraine needs Peace*, MKI Report - 2024, <https://hiia.hu/wp-content/uploads/2024/06/MKI-Report_After-Twenty-Seven-Months-of-War-Ukraine-Needs-Peace.pdf>
6. Kullab S., *Thousands of North Korean troops in Russia. What does that mean for the war with Ukraine?*, "AP News", October 31, 2024,

<https://apnews.com/article/russia-ukraine-north-korea-war-735ab717dcf92a718adcb68bfbddc653>
7. Lough J., *Four Scenarios for the End of the War in Ukraine*, Chatham House 2024, <https://www.chathamhouse.org/2024/10/four-scenarios-end-war-ukraine>
8. Paffenholz T., Bramble A., Poppelreuter P., Ross N., *Negotiating an End to the war in Ukraine: Ideas and Options to Prepare for and Design a negotiation process*, Report 2023
9. *President Zelenskyy Peace Formula - Ukraine's Peace Formula Philosophy*, <https://www.president.gov.ua/storage/j-files-storage/01/19/53/32af8d644e6cae41791548fc82ae2d8e_1691483767.pdf>
10. Santos S. F., *Trump ally says Ukraine focus must be peace, not territory*, "BBC News", November 9, 2024, <https://www.bbc.com/news/articles/czxrwr078v7o>
11. Stückelberger Ch., *Ukraine-Russia: Twelve Proposals Towards Negotiated Peace*, <https://www.fpablovi.org/images/Actualidad/firma/Ukraine-Russia.pdf>
12. Thompson Reuters, *Source says Trump advice Putin not to escalate Ukraine war, Kremlin denies conversation*, CBC.CA, November 11, 2024, <https://www.cbc.ca/news/world/trump-putin-phone-call-ukraine-1.7380033>
13. *Trump urges Putin to avoid escalation in Ukraine war, report says*, "France24", November 11, 2024, <https://www.france24.com/en/europe/20241111-trump-putin-ukraine>
14. Yakymenko Y. (ed.), *Ukraine from war to peace and recovery*, Razumkov Centre, Kyiv, September 2024

„Ante Portas – Security Studies”
2024, No. 21
DOI: 10.33674/1202425

Oliver B. STEWARD[1]
United Kingdom

THE KURSK ‘OFFENSIVE’, THE WAR OF MANOEUVRE, & MANAGED ‘ESCALATION’: AN ANALYSIS

Abstract: *This paper poses the central theme for researchers: What can military practitioners and strategic studies scholars learn about this military operation? The underlying strategic and political factors behind the (a) decision to launch the military operation? (b) in what way has the Ukrainian Armed Forces carried this out so far? However, two further factors need to be considered: (c) how this impacts the changing nature of the conflict, and (d) how the Russian Federation, and particularly President Putin’s leadership, responded. There has also been much debate about the concept of ‘managed escalation’, and the case study of the Kursk Offensive is one of ‘escalation’, within the context of the wider conflict. Did the Ukrainian Kursk Offensive, along with deep strikes, achieve the objectives of the Ukrainian Armed Forces? It is a testament to Ukraine’s military intelligence that this operation was carried out in the first place, in addition to how this has coincided with a calculated campaign of ‘deep surgical strikes’ of Ukrainian Drones into the Russian Federation, serving not just a strategic but also, a psychological imperative.*

Keywords*: Kursk, offensive, drones, escalation, Russia, Zelensky, strategy, military objectives, attritional, ICBM*

The Kursk offensive: a shift towards manoeuvre warfare

The Kursk 2024 spearhead on the 6th August 2024 was a significant moment in the conflict and one which had taken Moscow by surprise. The Ukrainians' use of elite mechanized forces, along with forward-deployed paratroopers and

[1] Oliver B. Steward, PhD, Royal Institute for International Affairs (UK), ORCID: 0009-0002-2854-2787, email: oliver.steward@outlook.com

air-assault units, meant that it was serious about this offensive. Traditionally, this war has been fought using attritional tactics, as I previously wrote in an article: "In operational terms, the Russian military in Ukraine has pursued a 'defence-in-depth' strategy that included fortifications and anti-tank mines"[2]. The use of 'Blitzkrieg' tactics, by flanking and encircling the Russian forces in the Kursk oblast demonstrated the superior nature of Ukraine's warfighting capabilities. However, the question posed is what is Ukraine's underlying military and political strategy concerning this offensive? Initially, it can be argued that Ukraine has pulled off a strategic and military masterstroke by launching this offensive.

Firstly, one must define what military strategy is. The standard definition can be defined as "ways" as well as ends and means (Lykke1989, 2-8)[3]. However, there is a wider strategic imperative at play. This is the acknowledgement by decision-makers in Kyiv that Ukraine is unable to win the brutal war of attrition, due to the numerically superior Russian forces. Therefore, the Ukrainian military leaders instead decided to take the fight to the Russian interior, and therefore regain the initiative. This offensive, also, provides 'maximal pressure' upon the Kremlin to react to the situation and divert resources away from other areas.

By comparing the 2024 spearhead to the failed offensive in 2023, one thing is very clear. This was very carefully coordinated and had momentum, with the use of superior forces, with a clear objective of seizing Russian territory, rather than skirmishes by pro-Ukrainian Russian Forces:

"First, it is a classical military offensive being carried out on a large scale by Ukraine's armed forces. Previous infantry raids into Russian state territory were carried out by small and semi-regular Free Russia Legion and Russian Volunteer Corps consisting of Russian citizens fighting on Ukraine's side. The recent land invasion into Russia, in contract, is carried out by large and regular mechanized and combined Ukrainian troops"[4].

From an operational military standpoint, an important distinction needs to be made:

"[T]he land warfare between Russia and Ukraine has, with [the] Kursk incursion, switched from a confrontation almost exclusively playing out on Ukrainian terrain to one now being fought on both countries' legal state

[2] O. Steward, *Russia's Embrace of Attritional Warfare: "Winning By Not Losing"*, "Proceedings" 2024, Vol. 2, No. 1, *Romania and the dynamics of international security*, <https://revista.unap.ro/index.php/XXI_NDC/article/view/2042> (23.12.2024).

[3] This quote was taken from my previous article, see: O. Steward*, Russia's Embrace..., op. cit.*

[4] A. Umland, *A Turn in the Russo-Ukrainian War?*, "Stockholm Centre for Eastern European Studies" 2024, No. 12, <https://www.ui.se/globalassets/ui.se-eng/publications/sceeus/2024-publications/a-new-turn.pdf> (23.12.2024).

territories"[5]. Furthermore, the report goes onto add the following: "It has already after the first days of its implementation become a source of embarrassment and distraction for the Kremlin". The strategic rationale can be summed up by stating that the "Kursk offensive, therefore, is also an attempt to deviate Russian forces out of the positional warfare and bring the war to Russia"[6].

Consequently, this has become less of a war of attrition, and more of a war of manoeuvre, and during the initial phase of the incursion led to the following observation by the author: "Kyiv's redirection of its defensive warfare onto Russian soil will have pragmatic as well as strategic and not only operational or tactical meaning"[7]. This is evidently seen in "With the Ukrainian troops' relatively deep incursion into Western Russia, the war has become less of an attrition" and instead one of 'manoeuvre'[8]. That being said, there is also a wider geo-strategic imperative. Therefore, in terms of the escalation, the political imperative of such a military operation can be seen in the following logic. The "Kursk operation appears to have been designed, in part, to destroy Western fears about the dangers of nuclear escalation"[9]. Russia has been attacked on its own territory and it hasn't used nuclear weapons. But Zelensky [has not] been able to translate the battlefield gain into changing Western leaders' mind"[10]. That changed in the coming months ahead, following the 2024 U.S. Presidential election. Therefore, it can be argued, that a changing political imperative, rather than solely a strategic imperative, was informing the Biden administration's thinking on the issue.

In addition, during his trip to the United Nations, on September 22nd-23rd, Ukrainian President Zelensky said to the United States, to present to President Biden his 'Victory Plan'. Therefore, one can conclude that at least from a political messaging standpoint, Zelensky is attempting to reframe the lack of battlefield momentum and inject a new narrative. Interestingly, Patrick Sullivan, writing for *The Modern War Institute at WestPoint,* argues the following:

"For the Ukrainians, the incursion is a proverbial shot in the arm that can undo some of their own war fatigue and bolster them to face whatever remains

[5] *Ibidem*.
[6] L. Johnson, *The Meaning of the Kursk Offensive*, "International Politik Quarterly" 2024, No. 4, <https://ip-quarterly.com/en/meanings-ukraines-kursk-offensive> (23.12.2024).
[7] A. Umland, *op. cit.*
[8] *Ibidem*.
[9] L. Johnson, *op. cit*.
[10] *Ibidem*.

in the current fighting season, as well as another winter without reliable electricity"[11].

The perspective in terms of the optics of the offensive for the Russians is as follows:

"[T]he incursion penetrates Putin's tightly controlled and highly curated narrative about the war. The war being brought to Russian doorsteps - beyond the missile and drone attacks that Ukraine prosecuted earlier this year in the Belgorod region – changes the stakes of the war, invites new contemplations on its possible outcome, and weakens Putin's image as the capable political leader and strong military commander Russians need to ensure their security"[12].

The following two Figures, (Fig. 1.1.) and (Fig. 1.2.) respectively, will demonstrate the changing nature of the battlefield. First, following the initial offensive with the incursion into the Kursk region and, also, the following Russian counterattacks later this year and how it contrasts.

Firstly, despite Ukraine making significant progress initially, the Russians have been able to mount a counter-offensive to reclaim parts of its territory. Later on, this year, we can see in (Fig 1.2.) that the Ukrainians are still able to control a sizeable part of its original controlled areas and will likely adopt a 'defence-in-depth' approach, as the Ukrainian Armed Forces fortify its positions, and dig in trench networks and other defensive perimeter while the Russians make incremental gains.

[11] P. Sullivan, *Wedge and Hedge: The Political Logic of Ukraine's Border Incursion*, The Modern War Institute 14th August 2024, https://mwi.westpoint.edu/wedge-and-hedge-the-political-logic-of-ukraines-border-incursion/ (23.12.2024).
[12] *Ibidem*.

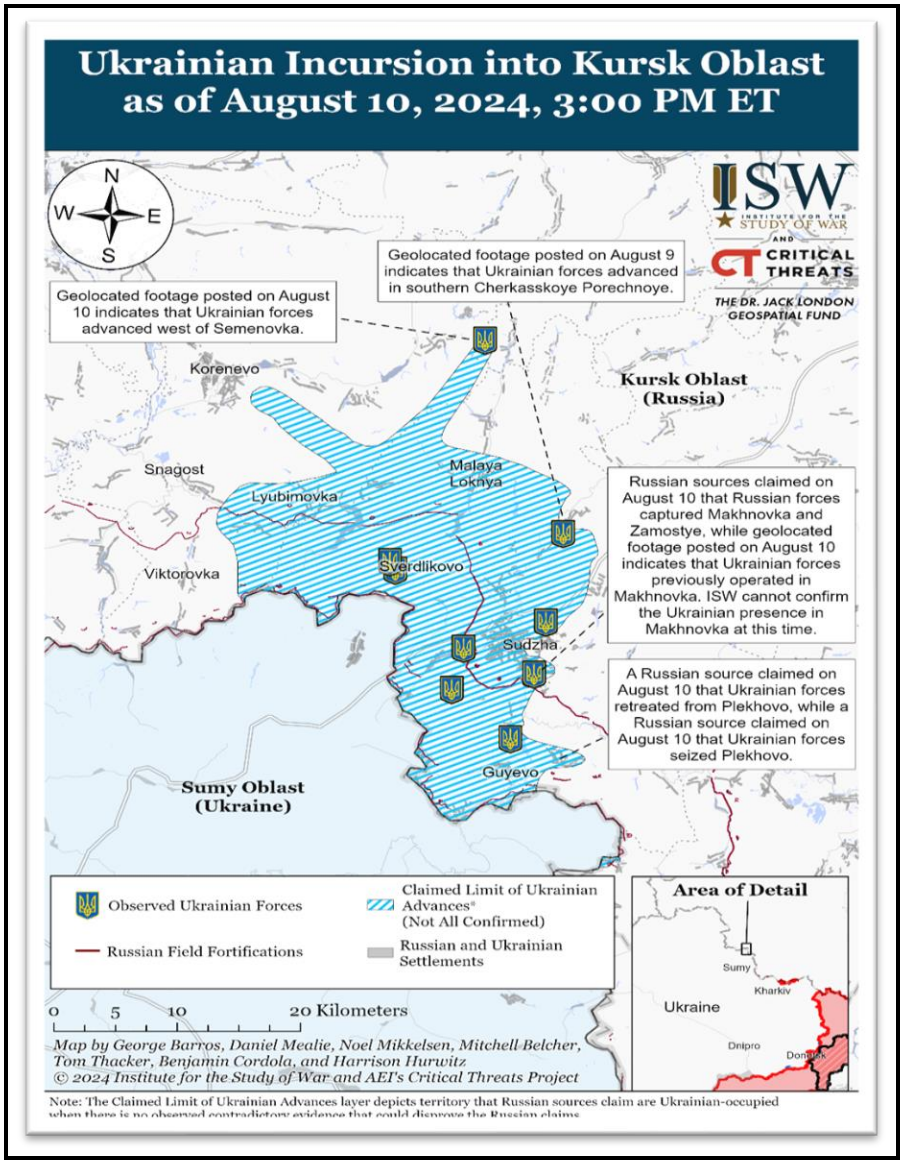

Fig. 1.1. Battlefield Map of the Kursk Offensive 10th August 2024, 3pm Eastern Standard Time[13]

[13] Institute for the Study of War, *Ukrainian Incursion into Kursk Oblast as of August 10 2024*, "ISW & Critical Threats Project" 2024, <https://www.understandingwar.org/sites/default/files/UAF%20Kursk%20Incursion%20August%2010%2C%202024.png> (23.12.2024).

It is also interesting to note that the *Institute for the Study of War* has stated that the "first North Korean forces likely officially engaged in combat against Ukrainian troops" by November 6th (date of Fig. 1.2).

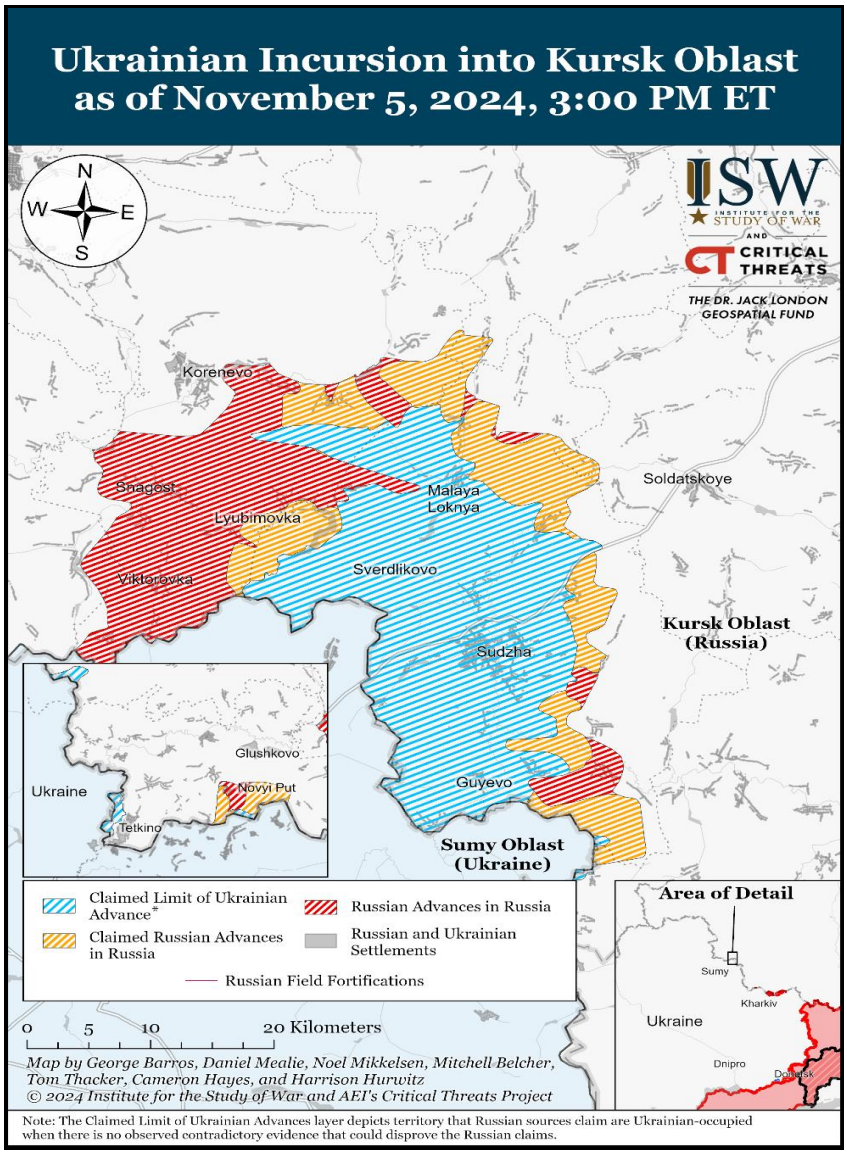

Fig. 1.2. Ukrainian Incursion into Kursk Offensive November 5th 2024, 3:00 pm Eastern Standard Time[14]

[14] Institute for the Study of War, *Ukrainian Incursion into Kursk Oblast as of November 5th 2024, 3:00 pm ET*, "ISW & Critical Threats Project", 5th November 2024,

Furthermore, it is difficult to establish who is North Korean and who is Russian, due to the North Korean troops being "disguised" as Russian soldiers. It therefore suggests that the "Russian military is trying to integrate North Korean combat power into the Russian force structure"[15]. This corroborates the claim that the Russians are using the North Korean troops as force multipliers to bolster their ranks. Furthermore, due to manpower shortages this will likely be expanded upon by the Russian military in an effort to maximise its firepower in the region.

Therefore, the strategy behind this military operation was clearer and more cohesive to increase Ukraine's bargaining position, as well as inflict a military and psychological blow to the credibility of Moscow and President Putin. Consequently, Ukrainian President Zelensky and his military commanders made a strategic move to open up another front, for Ukraine to regain the initiative and be back on the military offensive, on its terms.

In the operational context, the Ukrainian 'Blitzkrieg' had outwitted and out-maneuvered the Russians at every turn. Furthermore, this combined with Ukrainian 'drone' strikes, further demonstrated the increasingly chaotic scenes in the Russian Federation itself. For example, the Ukrainian paratroopers spearheading the assault were able to effectively surround and destroy Russian units in the interior – while also working in synchronicity with other Ukrainian units on the ground and in the air. Furthermore, the Ukrainian 'air assault' brigades had taken the initiative by utilising Western firepower in the form of British-made, Challenger II tanks as well as American-made Bradley and Stryker vehicles, with both having superior protection for the crew. Furthermore, the superior tactics employed by the Ukrainian Armed Forces on the ground did have a further impact of shifting battlefield momentum, towards the Ukrainians at the expense of the local Russian forces – who were unorganised, outflanked, and surrounded by crack elite forward Ukrainian paratroopers, air assault, and mechanised infantry.

The Kursk offensive was Ukraine's 'window of opportunity' that it had to exploit. The Kursk region provided good terrain to launch an effective offensive, and Ukrainian intelligence discerned that the Russian interior consisted of poorly trained conscripts and 'reserve' forces. However, it is also worth mentioning that the Kursk region has good sources of logistical transport, such as communications and rail lines. The capture of which has disrupted the

---

<https://www.understandingwar.org/sites/default/files/UAF%20Kursk%20Incursion%20November%205%2C%202024.png> (23.12.2024).

[15] Institute for the Study of War, *Russian Offensive Campaign Assessment*, "ISW Press", November 5th, 2024, <https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-november-5-2024> (23.12.2024).

Russian military logistical capabilities, and that, combined with Drone strikes, has disrupted Russian military supply lines.

One of the military objectives was to relieve the Ukrainian fighting in the Donbas, by taking the war to the Russian heartland. In addition, the Ukrainian offensive has led to 100,000 Russians being evacuated or have fled[16]. Consequently, this has placed tremendous strain on Russian local authorities and other government agencies, who already have limited resources to deal with such eventualities. No doubt, this added confusion has further compounded the initial military difficulties of the Russians.

The Ukrainian progress in its offensive can also be attributed to the sophisticated Western military equipment given by the West enhances crew survivability[17]. For example, the Challenger II tank was created in the 1990s and is extremely reliable and powerful with good armour protection and a rifled 120 mm main gun with an advanced fire control system in operation[18]. Therefore, in the context of Ukrainian armoured warfare operations, this provides a further advantage as.

From a military operational standpoint – as of December 2024, neither Ukrainians nor the Russians are withdrawing from the Donbas front, with Russia making incremental gains in the Avdiivka region, as well as recently during the Battle of Chasiv Yar. Importantly, one of the initial military objectives of the Ukrainians was to get the Russians to pull forces away from the Donbas region. However, this has not occurred.

Ukraine's 'deep strikes' into the Russian Federation: drones, ATACMS & Russian ICBMs

While the Kursk Offensive became the major development in the Summer Offensive, this was further complimented by the other, asymmetrical side of Kyiv's military machine - that of its drones. It is arguably the case, that the Ukrainian military is operating with superior military intelligence and can

[16] L. Harned, *From Kursk to Kursk: Putin's attempt to project an image as Russia's 'protector' has been punctured throughout his 25 years in power*, "The Conversation", 26th August 2024, <https://theconversation.com/from-kursk-to-kursk-putins-attempt-to-project-an-image-as-russias-protector-has-been-punctured-throughout-his-25-years-in-power-237105> (23.12.2024).

[17] *Ukrainian Challenger 2 crew reveal how British-supplied main battle tank saves lives*, "BFBS Forces News" 2024, <https://www.forcesnews.com/ukraine/ukrainian-challenger-2-crew-reveal-how-british-supplied-main-battle-tank-saves-lives> (23.12.2024).

[18] *Ukrainian Tank Crews on Pros and Cons of British Challenger 2 and Number of These Tanks still in Operation*, "Defense Express", 10th March 2024, <https://en.defence-ua.com/weapon_and_tech/ukrainian_tank_crew_on_pros_and_cons_of_british_challenger_2_and_number_of_these_tanks_still_in_operation-9790.html> (23.12.2024).

launch coordinated strikes deep behind 'enemy lines' in Russia, particularly at night, without any Russian countermeasures.

However, it is also worth mentioning that during the initial phase of the offensive, the West, including the United States, had still not permitted to use its long-range weaponry, including American-ATACMS and UK-French built Storm Shadows to hit targets deep inside Russia. However, it could be argued that Western strategic calculus has been based on 'escalation management', and not to unduly provoke the Russian Federation in making further escalatory moves, due to it being a nuclear weapons power.

Ukraine's spearhead in Kursk, as well as what this paper terms as the 'Drone Offensive' against Russian munitions, airbases, and energy storage facilities, has challenged the whole notion of 'escalation management'. Despite Russia's nuclear rhetoric, the Ukrainian offensive has challenged this very notion, and the drone strikes have served to cause further logistical disruption as well as being of detriment to Russia's warfighting capabilities.

Following the 2024 Presidential election, as well as the military difficulties the Ukrainians were encountering on the battlefield, combined with the uncertainty that came with the election victory of President-elect Trump's commitment to Ukraine, provided the political and strategic impetus to lift the 'ban' on the usage of Western-made weaponry, so that Ukraine can strike targets inside the Russian Federation. It is important to note that authorising Ukraine to use such weaponry will strengthen its ability to wage war against a numerically superior adversary, from an operational military perspective, but it is doubtful this would fundamentally change the tactical and strategic landscape due to the sheer numerical advantages that the Russians currently have at its disposal.

While this did prompt Russia to again engage in nuclear sabre-rattling rhetoric, as well as a revision of nuclear doctrine, so far, its escalation has been, 'managed', pun intended. However, Russia did launch two, non-nuclear ICBMs, at Ukrainian targets. This was the first use of intercontinental ballistic missiles in a war-fighting capacity. Arguably, this served a political imperative – that of President Putin demonstrating the political will to launch such a strike upon Ukraine, and to remind the West that Russia still possesses the capability, if not the intent, to strike using the full range of its conventional, long-range capabilities. But the symbolism of using a weapon system, that is designed specifically, to carry a nuclear payload has not been lost.

President Putin's path dependency in the Ukraine conflict: massive losses on both sides & the deployment North Korean troops in Kursk

A wider point has to be made as to how this offensive impacted international public opinion, but also, just as important, the credibility of Putin as the

"master strategist". As the Russian state was now seen as weak due to its intelligence failures to firstly, (a) predict this offensive in the first place, but also, (b) the initial lacklustre and uncoordinated response by the Kremlin. However, this does bring up the issue of what strategic options Putin has moving forward. Furthermore, what can be realistically predicted?

Firstly, after the initial shock of the military operation, the Kremlin ordered its frontline units away from the Ukrainian front to defend its interior, as well as Chechen forces, known as 'Kadyrovites', being redeployed. However, this had a wider political imperative which meant the Russians calling this a "counter-terrorist operation" and placing the control of forces with the Secret Service and the FSB. This indeed reflected the growing nervousness of the Kremlin to both manage the perception of the unfolding of events, by calling it a 'counter-terrorism operation'[19] and, shifting the burden of responsibility away from the military and, instead, towards the interior ministry.

While taking into consideration Ukraine's 'Kursk' offensive, one must also consider the military constraints as well as the resource limitations of the Russian Federation, in the Summer of 2024. As I stated last year, this conflict has shifted from that of manoeuvre to a war of attrition. This has resulted in massive losses in both equipment and manpower. This has produced further constraints on strategic options moving forward.

President Putin's decision not to escalate this, but instead, shift the bureaucratic momentum from the military and towards the interior ministry, is also a testament to the Kremlin acknowledging the institutional limits that it operates. President Putin's leadership style is one of micro-management, but also, he must also shift the burden of responsibility. As was the case in late 2022, President Putin cannot (1) initiate full-mobilization, as this would be an acknowledgement that the war is not going well, and there will likely be public resistance to such an idea. Furthermore, it will impact President Putin's political capital. Secondly, (2) not changing the operational military response would also encourage further gains by the Ukrainian military in the Kursk region, which would have a further negative impact on Moscow's credibility. Furthermore, the current 'attritional' phase of the conflict means that the Russian leadership is unable to launch a 'surge' of troops in the region – as it is still having to wage a brutal offensive in the Donbas. Moving considerable forces from this particular theatre of operations will cost the Russian military much-needed firepower. Therefore, a third option needs to be considered.

However, one must also take into consideration the tremendous amount of losses the Russians have encountered as a result of its 'Special Military

[19] D. Sabbagh, *As Ukraine's Kursk incursion forges on the stakes are rising for both sides*, "The Guardian", 15th August 2024, <https://www.theguardian.com/world/article/2024/aug/15/ukraine-kursk-incursion-russia-stakes-rising-for-both-sides> (23.12.2024).

Operation'. The Russian military casualty figures have exceeded 600,000 troops, although it may even be the case that this figure is much higher. This was quoted by President-elect Trump in his social media post, quoted as saying "where close to 600,000 Russian soldiers lay wounded or dead in a war that should never have started, and could go on forever"[20]. Russia in its latest offensive in the Donbas was losing 1,500 soldiers per day due to the savage nature of the conflict. That being said, one thing to bear in mind is that Kyiv's figures are not made public, and one can at least infer that it may be comparable to that of the Russian side. That being said, what we do know is that Kyiv is also experiencing 'manpower' issues, with pressure growing to reduce the conscription age to 18, with Kyiv resisting pressure to do so[21].

From a strategic and operational standpoint, the introduction of North Korean troops does demonstrate escalation and the changing dynamics of this conflict. That leads this paper to consider the North Korean 'option' as a force multiplier in an era of military constraints. Russia has become more dependent upon North Korean weaponry and firepower to wage this war of attrition. The Ukrainians by launching this offensive have changed the character of the conflict, at least in the Kursk theatre of operations, by once again waging a war of 'manoeuvre'. As the North Koreans are being sent to the frontlines, reports indicate that they have sustained hundreds of casualties, although the figure itself is hard to approximate, due to the lack of independently verified sources.

It is important to consider how well integrated these North Korean soldiers are with the Russian military. If they are not integrated at all, the Ukrainians can use this to their advantage on the battlefield. Also, in terms of this increasing 'path-dependent' relationship between Moscow, and North Korea – we will likely see further North Korean troops fill the ranks in the Kursk region, while Moscow provides technological, economic and military aid to Pyongyang. While it is not the mainstay of this paper, nonetheless one can speculate that Russia will further enhance North Korea's ballistic missile program, while the North Koreans continue to provide fresh troops and war materials to aid in Moscow's war efforts. In addition, likely, the North Korean regime will further reinforce its ranks with a further commitment of troops for a potential upcoming Russian offensive, whenever that will eventually occur.

From a military operational standpoint, the North Koreans do not have the battle experience that the Ukrainians, or for that matter, Russians have. Furthermore, there does seem to be a lack of coordination and fire support, and

[20] D. Trump, @realDonaldTrump, Truth Social, Dec. 8th 2024 post, <https://truthsocial.com/@realDonaldTrump/posts/113615912452824634> (23.12.2024).

[21] W. Murray, *Ukraine War Briefing: US urges Zelenskyy to lower conscription age to 18'*, "The Guardian", 28th November 2024, <https://www.theguardian.com/world/2024/nov/28/ukraine-war-briefing-us-pressure-on-zelenskyy-to-lower-conscription-age-to-18> (23.12.2024).

instead, the focus is on 'human wave' assaults in open terrain against heavily defended Ukrainian positions. There have even been reports of friendly fire incidents with North Korean troops killing at least six Chechen soldiers. Additionally, there have also been reports of language issues, with a lack of mutually understandable linguists available. This will likely, at least in the short term, further compound the fighting ability of the fresh North Korean replacements.

The Biden 'surge' in military & financial aid: enough to turn the momentum in Ukraine's favour?

Following President-elect Trump's Victory in the 2024 Presidential election, we have seen a renewed commitment by the Biden administration, limited in escalation but continuing in its longstanding commitment to Kyiv. This is seen in terms of financial aid, the agreement for Ukraine to use Western-made weapons to strike targets inside Russia itself, and a further aid package of weaponry, armoured vehicles and munitions to be given by the end of the Presidential term. While this is limited in scope, it will enable the Ukrainians to strike logistic targets, and also airfields and other munitions storage sites that will have a direct impact on the battlefield.

Allowing Ukraine to strike targets deep inside Russia is a form of 'strategic escalation', which has been subject to controversy and political commentary on the relative merits in addition to the risks associated with such a strategic move. On a wider geopolitical note, this has the intention, at least in the short term, to demonstrate to Moscow that, regardless of the outcome of the 2024 Presidential election, the United States remains committed to aiding Ukraine's defense. But this also serves a wider political imperative. It locks the future administration into at least agreeing in principle to continue this policy and creates a certain 'path-dependent logic' in this escalation ladder. No doubt this will generate wider strategic questions for the incoming Republican administration as to how best to conclude the war, but also the efficacy of the authorisation of long-range weapons. According to *The Hill,* As President-elect Trump has posted on social media, "I don't think that should be allowed", and further arguing that, "Why would they do that without asking me what I thought? I wouldn't have had them do that, I think that was a big mistake"[22]. While Trump has also suggested he may reverse the authorization for Ukraine to use American-made long-range weaponry, specifically the (ATACMS) long-range weapon system, it remains to be seen whether this will be carried into Presidential policymaking come

[22] B. Dress, *Trump says Russia-Ukraine peace may be harder than Middle East*, "The Hill", 16th December 2024, <https://thehill.com/policy/defense/5042314-trump-says-russia-ukraine-peace-may-be-harder-than-middle-east/> (23.12.2024).

January 20th, 2025, onwards. It is still very much open to speculation at this stage.

Conclusion

While Ukraine has seized on the military and strategic initiative, the question now is whether it has been able to follow through. The short answer is, surprisingly, no. Although it has been able to capitalise on its initial gains and adopt a more defensive position – it has not led to the complete collapse of the Russian lines. Furthermore, the Russians have been able, to a limited extent, to reinforce its position, as well as, launch strikes against Ukraine's interior. In short, the Ukrainians have been able to seize on limited gains, but this has not turned into a decisive victory. Rather, it has turned into limited gains. In addition, Russia has sought the deployment of North Korean troops to free up Russian forces to fight in the Donbas. Therefore, it is very unlikely that Ukraine has the current manpower or current military capabilities to push back against the sustained Russian onslaught, and this will likely mean Russia will continue to make incremental gains. It is worth noting that the Ukraine war is still predominately a war of 'attrition', and as such, Russia still has the numerical advantages in terms of raw military firepower and manpower available, even if it is being augmented by North Korean troops in the short-to-medium term. Therefore, the use of North Korean troops as a 'force multiplier' will likely continue for the foreseeable future, as the relationship between Moscow and Pyongyang as beneficiaries.

Another consequence of this offensive, and another critical development, is found in the use of North Korean soldiers who for the first time since the Korean War have been deployed in combat roles, and for the very first time, been used in warfighting on the European continent – which has both a strategic as well as a symbolic value. During the time of this writing, North Koreans have sustained hundreds of casualties, and many have questioned the combat effectiveness of these soldiers. Only time will tell whether the use of North Korean soldiers will translate into any substantial military gains in Kursk, as well as potentially over theatres of operations. That being said, Ukraine's strategic position in Kursk is likely to remain a key bargaining chip in any future political discussions as to how to end the war and will likely be leverage in any compromise with the Russian Federation.

BIBLIOGRAPHY:

1. Dress B., *Trump says Russia-Ukraine peace may be harder than Middle East*, "The Hill", 16th December 2024, <https://thehill.com/policy/

defense/5042314-trump-says-russia-ukraine-peace-may-be-harder-than-middle-east/>
2. Freedman L., *Strategic Fanaticism: Vladimir Putin and Ukraine", in War in Ukraine: Conflict, Strategy, and the Return of a Fractured World*, Edited by Hal Brands, Johns Hopkins University Press 2024, Project MUSE, <https://muse.jhu.edu/pub/1/oa_edited_volume/chapter/3881916>
3. Harned L., *From Kursk to Kursk: Putin's attempt to project an image as Russia's 'protector' has been punctured throughout his 25 years in power*, "The Conversation", 26th August 2024, <https://theconversation.com/from-kursk-to-kursk-putins-attempt-to-project-an-image-as-russias-protector-has-been-punctured-throughout-his-25-years-in-power-237105>
4. Institute for the Study of War, *Russian Offensive Campaign Assessment*, "ISW Press", November 5th, 2024, <https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-november-5-2024
5. Institute for the Study of War, *Ukrainian Incursion into Kursk Oblast as of August 10th, 2024*, "ISW & Critical Threats Project", 2024, <https://www.understandingwar.org/sites/default/files/UAF%20Kursk%20Incursion%20August%2010%2C%202024.png>
6. Institute for the Study of War, *Ukrainian Incursion into Kursk Oblast as of November 5th 2024, 3:00 pm ET*, "ISW & Critical Threats Project", 5th November 2024, <https://www.understandingwar.org/sites/default/files/UAF%20Kursk%20Incursion%20November%205%2C%202024.png>
7. Johnson L., *The Meaning of the Kursk Offensive*, "International Politik Quarterly", 2024, No. 4, <https://ip-quarterly.com/en/meanings-ukraines-kursk-offensive>
8. Lykke A., *Defining Military Strategy*, "Military Review" 1989, Vol. 69, No. 5
9. Murray W., *Ukraine War Briefing: US urges Zelenskyy to lower conscription age to 18*, "The Guardian", 28th November 2024, <https://www.theguardian.com/world/2024/nov/28/ukraine-war-briefing-us-pressure-on-zelenskyy-to-lower-conscription-age-to-18>
10. Sabbagh D., *As Ukraine's Kursk incursion forges on the stakes are rising for both sides*, "The Guardian", 15th August 2024, <https://www.theguardian.com/world/article/2024/aug/15/ukraine-kursk-incursion-russia-stakes-rising-for-both-sides>
11. Steward O., *A Lesson in Military Doctrinal and Operational Failures: The Battle of Hostomel and the Russian Military's Failure to Capture Kyiv*, "Proceedings" 2024, Vol. 2, No. 1: *Romania and the dynamics of international security"*, <https://revista.unap.ro/index.php/XXI_NDC/article/view/2041/1994>

12. Steward O., *Russia's Embrace of Attritional Warfare: "Winning By Not Losing"*, "Proceedings" 2024, Vol. 2, No. 1: *Romania and the dynamics of international security*, <https://revista.unap.ro/index.php/XXI_NDC/article/view/2042>
13. Sullivan P., *Wedge and Hedge: The Political Logic of Ukraine's Border Incursion*, The Modern War Institute, 14th August 2024, <https://mwi.westpoint.edu/wedge-and-hedge-the-political-logic-of-ukraines-border-incursion/>
14. Trump D., @realDonaldTrump, Truth Social, Dec. 8th 2024 post, <https://truthsocial.com/@realDonaldTrump/posts/113615912452824634>
15. *Ukrainian Challenger 2 crew reveal how British-supplied main battle tank saves lives*, "BFBS Forces News" 2024, <https://www.forcesnews.com/ukraine/ukrainian-challenger-2-crew-reveal-how-british-supplied-main-battle-tank-saves-lives>
16. *Ukrainian Tank Crews on Pros and Cons of British Challenger 2 and Number of These Tanks still in Operation*, "Defense Express", 10th March 2024, <https://en.defence-ua.com/weapon_and_tech/ukrainian_tank_crew_on_pros_and_cons_of_british_challenger_2_and_number_of_these_tanks_still_in_operation-9790.html>
17. Umland A., *A Turn in the Russo-Ukrainian War?*, "Stockholm Centre for Eastern European Studies" 2024, No. 12, <https://www.ui.se/globalassets/ui.se-eng/publications/sceeus/2024-publications/a-new-turn.pdf>

„Ante Portas – Security Studies”
2024, No 21
DOI: 10.33674/1202426

Eka BERAIA[1]
Georgia
Mariam DALAKISHVILI[2]
Georgia

INTERCULTURAL DIALOGUE IN POSTMODERN SOCIETIES AND ITS POLITICAL IMPLICATIONS – GEORGIAN CASE

Abstract: *This article deals with the topic of intercultural dialogue in postmodern societies and discusses its political implications particularly focuses on the case of Georgia, and analyzes the extreme importance of intercultural dialogue in today's diverse, multifaceted and closely interconnected world. In today's era of globalization, migration and digital communication, it is vital to reflect on the role of intercultural dialogue and understand its essence, although we should not forget that in the past, cultures were isolated and even seemed to exist in vast spaces. Now the reality is completely different, cultures today coexist and interact more closely than ever, which makes intercultural dialogue a crucial tool for promoting understanding and inclusion. The political implications of intercultural dialogue seem particularly interesting because, on the one hand, it has the power to positively influence policy areas, prepare political basis for immigration into the country, to impact the education system, and also to balance social integration by promoting inclusive approaches. Moreover, intercultural dialogue encourages the emergence and intersection of identity issues with politics and nationalism, which can strengthen or weaken social cohesion. These are the issues that the world is currently facing and it is trying to understand what is the role and power of intercultural dialogue, which in some cases acts in such a way as to trigger nationalist sentiments in societies or provoke resistance from societies that do not want to participate in cultural exchanges at all and even distance themselves from these processes. It is precisely the phenomenon that has to be studied and analyzed as its tension and ambiguity is important today. It is precisely this question that is essential to answer today: can intercultural*

[1] Eka Beraia, PhD, Caucasus International University (Georgia), email: eka.beraia@ciu.edu.ge
[2] Mariam Dalakishvili, MA, Caucasus International University (Georgia),

dialogue bring political stability to the country or not. As for Georgia, it is a multi-ethnic society, as it is a country located at the crossroads of Eastern Europe and Western Asia. Therefore, it is logical that the importance of intercultural dialogue is particularly noticeable in Georgia, as it is a country that has chosen the path of Western integration, including the aspiration to the European Union and NATO, poses unique challenges, because only in this way is it possible to balance minority rights, social cohesion and national identity. By analyzing the opportunities and challenges facing Georgia, the article aims to create a framework for understanding the complex role of intercultural dialogue in modern politics and society[3].

Keywords: *intercultural dialogue, postmodern, societies, globalization, migration, politics, communication*

Introduction

Postmodernism, which emerged in the late 20th century, is a philosophical and cultural movement that challenges deeply held norms and unique truths. It is characterized by skepticism and distrust of narratives of both religious and scientific, political ideologies - all-encompassing explanations, such as religion, science, or ideology, that claim to provide absolute truths about the world. Postmodernism rejects such claims, arguing that these are superficial "truths" and are socially constructed, often serving the interests of dominant groups while marginalizing others. For postmodernism, social values are presented in a completely different way[4]. It supports pluralism and believes that many identities, beliefs, and different worldviews can coexist harmoniously without any hierarchy. This is why it is clear why postmodernism recognizes diversity and rejects the imposition of any strict cultural-moral standards. And gives priority to practical considerations derived from one's own experiences[5]. This philosophical position promotes a more fragmented, decentralized view of society, where individuals and communities create their own meanings and values. The essence of postmodernism is inter-culturalism. It is a unique method, perspective, and approach to building and strengthening the unity of

[3] J. Applegate, H. Sypher, *A Constructivist Outline*, [in:] W. Gudykunst (ed.), *Intercultural Communication Theory - Current Perspectives*, "International and Intercultural Communication Annual" 1993, Vol. VII, Beverly Hills: Sage.

[4] J. K. Burgoon, A. S. Ebesu Hubbard, *Cross-cultural and intercultural applications of expectancy violations theory and interaction adaptation theory*, [in:] W. Gudykunst (ed.), *Theorizing about intercultural communication*, Sage 2009, pp. 149-171.

[5] *Ibidem.*

society. It is a theoretical framework that emphasizes dialogue, cooperation, interaction, and mutual understanding between cultures. Here it is necessary to clearly define and distinguish what distinguishes multiculturalism from interculturalism[6].

Theoretical framework

Unlike multiculturalism, which is often focused on the coexistence of different cultural groups with minimal interaction, and supports the exchange of ideas and integration into society. Interculturalism helps and encourages societies to cope with the challenges of diversity by tolerating differences, respecting cooperation over segregation, and seeking a balance between cultural inclusivity and fostering common ground. This highlights the importance of adaptation and openness in building inclusive and dynamic societies. It is a key instrument r that paves the way for modern societies to cope with the challenges of globalization and diversity[7].

As for dialogue, it can be said that it is the main axis of human communication, which serves as a bridge between individuals and cultures and establishes a close connection between them. This form of dialogue is supported by philosophical theories, especially those of Hans-Georg Gadamer and Martin Buber, according to which the methodology and theoretical framework of how we interact with others and the world around us, are formulated and explained[8]. These theories not only provide the key to understanding human interaction, but also they remain relevant in the context of intercultural exchange in modern societies. Hans-Georg Gadamer's theory emphasizes the importance of dialogue in the process of understanding and interpretation. Gadamer argues that understanding cannot be considered a simple activity, but rather a process that occurs through interaction - an ongoing interpretive conversation, for example, between an interpreter and a speaker or between a text that carries specific information. In his view, when individuals from different backgrounds engage in dialogue, they interpret and create new possibilities, one might say new understandings, that go beyond individual perspectives. In intercultural exchange, Gadamer argues that people from different cultural backgrounds can engage in a dialogical process that makes understanding more diverse and interesting. For example, when two people

[6] L. A. Samovar, R. E. Porter, *Communication Between Cultures* Wadworth 20, Channel Street, Boston MA 02210 US Eight Edition 2021.

[7] T. Antenehm, *An integrative approach to intercultural communication in context: empirical evidences form higher education*, Giessen, 2019, pp. 1-132.

[8] J. Cohen, *Form and Content in Buber's and Schweid's Literary-Philosophical Readings of Genesis*, "Religions" 2019, No. 10(6), pp. 398–410.

from different cultures speak, each person's cultural horizon is broadened as they try to understand the other's experiences, beliefs, and values.

The process of dialogue becomes a tool for overcoming misunderstandings and achieving a common understanding, which is crucial in today's multicultural societies. Martin Buber's philosophy, or the concept of the "I-Thou" relationship, offers another philosophical justification for the essence and nature of dialogue[9]. Buber distinguishes between two categories of interaction: the "I-It" and the "I-Thou" relationship. In the first, the "I-It" encounter is ego-centric, a separate, individualized experience, as if interpreted from another lens or dimension. In contrast, the "I-Thou" relationship is a genuine encounter, where individuals engage with each other as individuals, not as mere objects or tools. This encounter is characterized by high social activity, openness, mutual respect, and the recognition of the other as a fully human being. In the context of intercultural dialogue, Buber's theory suggests that true understanding can only occur when individuals approach others from a place of equality, openness, and respect. When people from different cultures engage in "I-Thou" relationships, they come to know each other not only as members of their own culture, but also as people who can break stereotypes and prejudices. Such dialogue allows for the recognition of a common humanity and fosters empathy, making it an important tool for promoting peaceful intercultural exchange in modern societies[10].

According to the works of Gadamer and Buber, the theory of dialogue, is not just a simple everyday conversation or exchange of information. It is a rather complex transformational communication, an interpretive and relational interaction that requires openness, respect and mutual engagement, the process of interpretation being engaged in a dialogue, where understanding is both shared and simultaneously created, while Buber's "I-Thou" relationship emphasizes the ethical, relational and fully human nature of authentic dialogue. Therefore, the above theories develop a deep understanding of how meaningful conversations shape our relationships and our understanding of the world and others.

What difficulties can Georgia overcome through intercultural dialogue?

Georgia, despite its small population and area, occupies a strategic position with direct access to the Black Sea and Turkey. The USA policy changes

[9] H.-G. Gadamer, *Sections of Truth and Method*, Second, Revised Edition, Translation revised by J. Weinsheimer, D. G. Mars, London and New York, Continuum 2004, https://mvlindsey.files.wordpress.com/2015/08/truthand-method-gadamer-2004.pdf (14.10.2024).

[10] J. Cohen, 2019. *Form and Content in Buber's and Schweid's Literary-Philosophical Readings of Genesis*, "Religions" 2019, No. 10(6), pp. 398–410.

alleviate the vulnerability of the mission's geo-economic interests in the region, but this often comes with trade-offs such as Russian involvement, weak democracies, and Islamist influence, which hinder Georgia's democratic development and threaten its independence and territorial integrity. Georgia's historical past, geographical location, and political landscape have shaped its unique cultural and social reality, which is now part of the Georgian diaspora. The country is located in the South Caucasus, bordered by Russia to the north, Turkey and Armenia to the south, and Azerbaijan to the southeast. It has a rich history of interaction and coexistence among its unique multicultural, multi-ethnic, and multi-religious groups, which has influenced the formation of its interesting, multi-faceted national identity. Intercultural dialogue in Georgia is therefore essential to overcome the divisions between the ethnic Georgian majority and minority groups, of which the country has a rich experience[11]. The country has experienced significant ethnic tensions and internal conflicts, particularly in the regions of Abkhazia and South Ossetia, which are now occupied by the Russian Federation (it should be mentioned that the loss of these territories were the result of the conflict, inspired by the Russian Federation in Georgia and the subsequent bloody inter-ethnic war led to the suspension of the dialogue). The point is that in these separatist regions, ethnic Georgians were forcibly displaced and the local Abkhazian and Ossetian populations were involved in conflict with Georgian forces. These unresolved conflicts continue to influence political discourse in Georgia and require intercultural dialogue to address issues of ethnic identity, self-determination, and territorial integrity[12]. In the post-Soviet context, intercultural dialogue can become a tool for rebuilding trust, promoting reconciliation, and creating a framework for peaceful coexistence, although political realities and Russian influence complicate the situation up to now. Georgia's geopolitical location has placed it in a zone of tension and competition between Russia and the West, especially since the country declared independence from the Soviet Union. Moreover, the military presence in Georgia's breakaway regions of Abkhazia and South Ossetia has raised questions about national sovereignty, security, and the role of intercultural dialogue in peace building. The August 7, 2008 is considered to be a drastic date for Georgians as brutal Russian military forces advanced ahead and invaded part of Georgia. The conflict itself was over in

[11] L. Bryant, *As Anti-War Russians Flock to Georgia, Tbilisi Warms to Moscow*, Voice of America 2023, <https://www.voanews.com/a/as-anti-war-russians-flock-to-georgia-tbilisi-warms-to-moscow-/7133090.html> (14.10.2024).

[12] E. Sepashvili, *Deep and Comprehensive Free Trade with the EU: Dynamics and Prospects for Deeper Integration*, "Kiev National Economic University Proceeding" 2018, No. 1 (1).

several days, but the consequences were severe[13]. The above mentioned war could change not only the geopolitical environment, political reality but it had a great impact on the further movement of migrants not only in inter-boarder scale but it also trigger new flow of migrants across border[14]. Therefore, intercultural dialogue is particularly relevant here, as it provides a way to resolve tensions between Georgians and their sister nations, recognizing historical grievances and national aspirations. Regarding the need for cultural dialogue in the Georgian integration region, Georgia is home to a significant number of ethnic minorities, including Armenians, Azerbaijanis, Kurds, and, following the 2022 war in Ukraine, Russians and Ukrainians who immigrated. These communities often face challenges in terms of integration and recognition in Georgian society. Promoting intercultural dialogue is vital for social cohesion, ensuring that minority groups are heard and represented in the political and cultural landscape. It is also worth noting that the Georgian language remains a critically important issue for the integration of minority communities. Although Georgian is the official language, many minorities speak their native language at home. This naturally creates certain challenges and difficulties, including for the non-Georgian population in accessing education, employment and full participation in the democratic process. Promoting multilingual education and policies that foster intercultural understanding can contribute to greater inclusion and political stability[15].

Multicultural Dialogue in a Religious and Political context

Religion is very influential in the reality of Georgia, Georgia is a country that adopted Christianity back in 337 and since that day this religion is considered the state religion. The Orthodox Church plays an important role in the culture and politics of the nation, influencing various aspects of public life. As the dominant religious institution, the Church often shapes national identity, public values, and social norms. Its influence is especially noticeable on the political landscape of the country, where it has historically been intertwined with nationalist sentiments, which provides a sense of unity and continuity for the Georgian people, especially in the context of post-Soviet state-building[16]. However, Georgia is also home to various religious minorities, including Muslims, Catholics, and Jews, whose participation in national dialogue is

[13] A. Silagadze, T. Zubiashvili, *Parameters of the European Union and the Post-Soviet Georgia's Economy*, "International Journal of Multidisciplinary Thought" 2015, No. 5 (3).
[14] T. Antenehm, *op. cit.*, pp. 1-132.
[15] M. Katamadze, *What Happened with Georgia's NATO Ambitions?– DW – 07/12/2023*, Dw.Com. <https://www.dw.com/en/what-happened-with-georgias-nato-ambitions/a-66190054> (14.10.2024).
[16] *Ibidem*.

essential for the development of a pluralistic society. These communities have their own historical and cultural significance, but they have sometimes faced challenges related to integration and recognition within the Orthodox majority context. Intercultural dialogue is therefore crucial for these minorities to feel valued and heard within the broader social realities of Georgia. In this context, intercultural dialogue is essential to foster tolerance, understanding, and peaceful coexistence across religious divides[17]. As a post-Soviet, post-modern society, Georgia is gradually moving towards greater secularism. This secular trend, coupled with the country's modernization, is calling into question the dominant role of the Georgian Orthodox Church in public life. Intercultural dialogue can be a vital tool to balance the significant influence of the Orthodox Church with the rights and representation of other religious communities, thereby creating a more inclusive environment where all groups can coexist harmoniously. This dialogue will not only emphasize the religious rights of minorities, but will also promote mutual respect and understanding.

Furthermore, since the early 2000s, European integration and full membership of the EU family have become a central political goal for Georgia. Georgia has sought closer ties with the European Union (EU) and NATO, in the hope that this will provide both economic growth and political stability. This aspiration has led to an acceleration of political and social reforms as Georgia aligns itself with European standards of governance, human rights, and democratic values. The EU promotes intercultural dialogue as one of the main pillars of its broader integration policy. For Georgia, EU membership requires not only economic and political adjustments, but also the promotion of greater intercultural understanding and the elimination of social divisions within its borders. These divisions are often linked to issues of ethnicity, religion, and regional autonomy, and they pose significant challenges to social cohesion. Unfortunately, in December 2024, the Georgian government, without any justification or reasoned explanation, suspended the initiative to join the European Union and violated the framework of the Association Agreement[18]. This has caused outrage among the Georgian population and, in the meantime, Georgia is still in a very difficult political phase, which also complicates the desire to open a dialogue with the peoples of European countries. Finally, intercultural dialogue plays a crucial role in Georgia's political and social transformation. As the country navigates the complexities of post-Soviet transition, geopolitical tensions, and domestic challenges, dialogue serves as a bridge to ensure that all groups, regardless of ethnicity, religion, or political affiliation, can engage in building a more peaceful and cohesive society. Georgia's efforts toward European integration, if successful, will largely

[17] L. Bryant, *op. cit.*
[18] M. Katamadze, *op. cit.*

depend on its ability to address these internal challenges and create a social environment where dialogue and cooperation are prioritized[19]. Through intercultural dialogue, Georgia can work to build a more democratic, pluralistic society, aligning its political practices with the European ideals of equality, tolerance, and mutual respect.

Conclusion

The existence of intercultural dialogue in postmodern Georgia is a multifaceted and vital process that holds the key to resolving the complex political, social, and ethnic tensions that affect the country's geopolitical, social, cultural, political, and religious realities. In the face of challenges such as territorial disputes, diverse ethnic and religious communities, and external geopolitical pressures, promoting dialogue between different groups is crucial for building a more inclusive, democratic, and peaceful society[20]. As Georgia continues its path toward stability and development, intercultural dialogue offers a transformative opportunity to bridge divides, foster understanding, and reconcile differences. By prioritizing communication between different ethnic, religious, and political factions, Georgia can better manage internal conflicts and create a cohesive national identity that reflects the diversity of its population. The case of Georgia highlights the importance of intercultural understanding not only for resolving conflicts but also for promoting lasting national unity[21]. Such dialogues provide opportunities where different groups can express their opinions, concerns, break down existing stereotypes, and work towards solutions that represent the interests of all citizens. Furthermore, promoting uniqueness and inclusiveness, as well as social cohesion through intercultural dialogue, ensures the fairness of political and social systems and the development of free societies[22]. In this way, Georgia can strengthen its democratic institutions and create a more sophisticated political culture based on respect, tolerance, and shared goals. This approach could also alleviate external pressures, allowing Georgia to pursue its aspirations for integration with the European Union and the broader international community, while preserving its cultural heritage and sovereignty.

---

[19] M. Cecire, *Georgia's Alliance With – Not In - NATO: External Balancing, Autonomy and Community*, [in:] T. German, S. Jones, K. Kakachia (ed.), I. B. Tauris (ed.), *Georgia's Foreign Policy in the 21st Century: Challenges for a Small State*, I. B. Tauris 2023.
[20] A. Silagadze, T. Zubiashvili, *op. cit*.
[21] E. Sepashvili, *Deep and Comprehensive …*, *op. cit.*
[22] E. Sepashvili, *Challenges of Innovative Policy for Eastern European Countries*, "Economics and Business" 2018, No. 11 (2).

BIBLIOGRAPHY:

1. Antenehm T., *An integrative approach to intercultural communication in context: empirical evidences from higher education*, Giessen, Germany 2019
2. Applegate J., Sypher, H., *A Constructivist Outline. In Gudykunst*, [in:] B. William (ed.), *Intercultural Communication Theory - Current Perspectives*, "International and Intercultural Communication Annual" 1993, Vol. VII, Beverly Hills: Sage
3. Beraia E., *Migration Problems at the Regional Security Level: Reasons for Georgian Migration Abroad*, "Białostockie Studia Prawnicze" 2021, Vol. 26, nr 1
4. Boyd M., *Family and Personal Networks in International Migration: Recent Developments and New Agendas*, "International Migration Review" 1989, No. 23 (3)
5. Broverman F. E., Inge K., Raymond S., Vogel, D. M., *Sex-role stereotypes: A current appraisal*, "Journal of Social Issues" 1972, No. 28
6. Bryant L., *As Anti-War Russians Flock to Georgia, Tbilisi Warms to Moscow*, Voice of America 2023, <https://www.voanews.com/a/as-anti-war-russians-flock-to-georgia- tbilisi-warms-to-moscow-/7133090.html>
7. Burgoon J. K., Ebesu Hubbard A. S., *Cross-cultural and intercultural applications of expectancy violations theory and interaction adaptation theory*, [in:] W. Gudykunst (ed.), *Theorizing about intercultural communication*, Sage 2009
8. Cecire M., *Georgia's Alliance With – Not In - NATO: External Balancing, Autonomy and Community*, [in:] T. German, S. Jones, K. Kakachia (ed.), *Georgia's Foreign Policy in the 21st Century: Challenges for a Small State*, I. B. Tauris 2023
9. Cohen J., *Form and Content in Buber's and Schweid's Literary-Philosophical Readings of Genesis*, "Religions" 2019, No. 10 (6)
10. Europeans Remain Welcoming to Immigrants, "The Economist" 2018, <https://www.economist.com/graphic-detail/2018/04/19/europeans-remain-welcoming-to-immigrants>
11. Gadamer H.-G., *Sections of Truth and Method*, Second, Revised Edition, Translation revised by J. Weinsheimer, D. G. Mars, London and New York, Continuum 2004, <https://mvlindsey.files.wordpress.com/2015/08/truthand-method-gadamer-2004.pdf>
12. Gečienė-Janulionė I., *Migration and Welfare State: The Coherence Between Welfare State, Migratory Regimes and Migration Flows*, "Filosofija. Sociologija" 2018, No. 29 (4)
13. Gibaldi J., *MLA Handbook for Writers of Research Papers*, New York: Modern Language Association 2009

14. International Organization for Migration (IOM) 2021 ”Year to review” Georgia Tbilisi-0162, Webpage: georgia.iom.int 13. Article 3 of the UN Protocol (2017, November): to *Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention Against Transnational Organized Crime*, <http://www.unodc.org/unodc/en/crime_cicp_convention.html>
15. Janušauskienė D., 2018. ‘We do not Need this Chaos: Attitudes of the Lithuanian People Towards Refugees’, “Filosofija. Sociologija” 2018, No. 29 (4)
16. Kerwin D., *International Migration and Work: Charting an Ethical Approach to the Future*, “Journal on Migration and Human Security” 2020, No. 8 (2)
17. Katamadze M., *What Happened with Georgia’s NATO Ambitions?– DW – 07/12/2023* <https://www.dw.com/en/what-happened-with-georgias-nato-ambitions/a-66190054>
18. Lee E. S., *A Theory of Migration*, “Demography” 1966, Vol. 3, No. 1
19. Ramachandran P. P., *The Methodology of Research in Philosophy. Chennai: Radhakrishnan Institute for Advanced Study in Philosophy*, University of Madras 1984
20. Ravenstein, E. G., *The Laws of Migration*, “Journal of the Statistical Society of London” 1885, No. 2
21. Reilly W., *Methods for the Study of Retail Relationships* Austin, TX: Bureau of Business Research, University of Texas 1999
22. Rorty R., *Philosophy as a Kind of Writing: An Essay on Derrida*, “New Literary History” 1978, Vol. 10, No. 1
23. Samovar L. A., Porter R. E., *Communication Between Cultures*, Wadworth 20, Channel Street, Boston MA 02210 US Eight Edition 2021
24. Sepashvili E., *Challenges of Innovative Policy for Eastern European Countries*, “Economics and Business” 2018, No. 11 (2)
25. Sepashvili E., *Deep and Comprehensive Free Trade with the EU: Dynamics and Prospects for Deeper Integration*, “Kiev National Economic University Proceeding” 2018, No. 1 (1)
26. Shioshvili T., *American Ethnicity*, Tbilis Black Sea Univerisy Publishment 2016
27. Silagadze A., Zubiashvili T., *Parameters of the European Union and the Post-Soviet Georgia’s Economy*, “International Journal of Multidisciplinary Thought” 2015, No. 5 (3)
28. Snow D. M., *National Security For A New Era: Globalization and Geopolitics*, Pearson Longman, New York 2004
29. *The Laws of Migration*, “Journal of the Statistical Society of London” 1885, Vol. 48, No. 2

30. *The Laws of Migration*, "Journal of the Royal Statistical Society" 1889, Vol. 52, No. 2
31. *The Birthplace of the People and the Laws of Migration*, "The Geographical Magazine" 1876, Vol. 3
32. Tukhashvili M., *Retrospective Comprehension of Post-Soviet Georgia's Population Migration*, "Georgian National Academy Bulletin" 2018, No. 12 (1)
33. UNICEF, UNHCHR, OSCE/ODIHR (2002, JUNE), "Trafficking in Human Beings in Southeastern Europe", <https://www.osce.org/odihr/18540?download=true>
34. *Trafficking in Persons report*, US Department of State 2003, <http://www.state.gov/g/tip/rls/tiprpt/2003/>

II. REVIEWS

„Ante Portas – Security Studies”
2024, No. 21
DOI: 10.33674/1202427

Piotr GIL[1]
Poland

ANDREW W. NEAL, *SECURITY AS POLITICS: BEYOND THE STATE OF EXCEPTION*, EDINBURGH UNIVERSITY PRESS, EDINBURGH 2020, PP 288

For anyone who follows attentively the scientific output within the field of security studies in the span of at least the last three decades and the former's constantly growing complexity across all the domains, levels, and manifestations of security issues, the notion that ever since the outset of broadening of the security agenda in the 80s of the XX century scholars have acquired a firm grasp of the essence of the phenomenon of security must seem indeed very compelling. Yet, the nature of security never ceases to baffle its students as it continues to pose an intellectual conundrum to those who seek to fathom it. Some have voiced that opinion by defining security as 'an ambiguous symbol'[2] or 'a contested concept'[3]. In their daily endeavours scholars face an array of fundamental questions pertaining to security, such as: what is security? What does it mean for a subject to be secure? how does security come about? Is security politics compatible with democracy? Those are but a few of the numerous questions that must be addressed before any security issue can be studied. In essence, it is the knot of the ontology of security that must be cut.

This is particularly the case with the theory and also the tangible and practical phenomenon of securitization. Over the years, the securitization theory has been substantially amended and enriched by scholars who addressed its shortcomings, supplemented it with new vital aspects, and pointed to new

[1] Piotr Gil, MA, Józef Goluchowski University of Applied Sciences in Ostrowiec Świętokrzyski, WSB University in Dąbrowa Górnicza (Poland).
[2] A. Wolfers, *"National Security" as an Ambiguous Symbol*, "Political Science Quarterly" 1952, Vol. 67, No. 4, pp. 481-502.
[3] B. Buzan, *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Colchester 2016, p. 216.

avenues for research[4]. However, it seems hardly possible to ascertain that, as a result of their efforts, it has been conclusively determined what it means that something has been securitized, i.e. it has become a security issue. More precisely, what remains obscure is, for instance, the difference between the areas of security and 'normal' governmental politics, especially in democratic and law-abiding countries. As per the fundamental tenets of the securitization theory, when security is invoked concerning an issue that is to become securitized, that issue gets "lifted above politics"[5] and "extraordinary measures"[6] are employed to tackle the threat to the referent object[7]. Does this mean, however, that the act[8] of securitization drives a wedge between the realms of politics and security, causing a complete disjunction between them? Is security not one of the aspects of social life and one of the policies that are governed by politicians and through politics? Those and many more questions are taken up by Andrew W. Neal in his book entitled "Security as Politics: Beyond the State of Exception", in which he challenges the outlook on the nature of security as a social and political phenomenon and the relation between security and politics, represented by the Copenhagen School and being an intrinsic part of the securitization theory.

In light of the securitization theory and other concepts developed within the much broader confines of critical security studies, one could point out three levels at which social issues can be considered. On top of the levels of politics and security, there is also the level of risk. If a social issue is subject not to securitization, but what Olaf Corry termed 'riskification', then, in short, it is not subsumed under the rubric of threat that is to be feared and dealt with the use of extraordinary measures, but treated as a risk and challenge that can be

[4] The literature whose authors aimed to amend and build upon the original securitization theory developed by the Copenhagen School is so extensive that it would be impossible to provide even a rough overview of it, especially when it comes to the papers published in journals. Therefore, only a few books of central importance have been adduced here. See T. Balzacq, *Securitization Theory: How Security Problems Emerge and Dissolve*, London 2011; H. Stritzel, *Security in Translation: Securitization Theory and the Localization of Threat*, Basingstoke 2014; J. Huysmans, *The Politics of Insecurity: Fear, Migration and Asylum in the EU*, Abingdon 2004; R. Floyd, *The Morality of Security: A Theory of Just Securitization*, Cambridge 2019; J. Hagmann, *(In-)Security and the Production of International Relations: The Politics of Securitization in Europe*, Abingdon 2014; H. Broecker, *Securitization as Hegemonic Discourse Formation: An Integrative Model*, Munich 2022.

[5] B. Buzan, O. Wæver, J. de Wilde, *Security: A New Framework for Analysis*, Boulder 1998, p. 26.

[6] Ibid, p. 21.

[7] Ibid, p.36.

[8] According to some authors, it is more apt to perceive securitization as a process or a set of institutionalized practices. See H. Broecker, *Securitization…*, op. cit., pp. 34, 38, 99.

controlled and managed[9]. The main advantage of this approach is that it allows us to comprehend the nature of security (issues) more comprehensively by going beyond security and politics being pitted against one another to form an alternative that often turns out to be out of touch with the reality. However, Andrew W. Neal points out the potential downside of introducing the logic or risk (management) into security politics, i.e. riskification. Following Jonas Hagmann and Myriam Dunn Cavelty[10], he claims that "the way risk analysis favours experts once security politics also has implications for traditional security politics. Its scientificism undermines the sovereign decisionism traditionally associated with security because it hinders the symbolic leeway of political leaders to represent threats and risks."[11] There seem to be two sides to sides coin. On the one hand, having political leaders make decisions based on substantive rather than emotional or ideological arguments is undoubtedly preferable. On the other hand, though, in democratic countries, the responsibility for making security-related decisions rests with political leaders and therefore it is their judgment that should take precedence over that of the experts, not the other way around. The experts' professional and scientific knowledge is very often invaluable when an important decision regarding national security (or just any of its branches) is to be made, but ultimately, their role is and should remain auxiliary in countries that are democracies and not technocracies. Neal's advocacy of the 'politicisation' of security is an important reminder of this fact.

As far as securitization and politicization of social issues are concerned, an irresistible question arises: why treat security as the negation of politics even though the empirical evidence proves undeniably that there is no state and no government without (national) security politics, which is not only not (much) different from other branches of politics, but also overlaps with them? To realize and acknowledge this more easily, it is helpful to adopt the epistemological and methodological perspective of Foucault's empirical historicism and problematization of security, elaborated by Neal, who believes that for one to be able to accurately grasp the nature of security it is essential to treat is a volatile and dynamic phenomenon, whose meaning is derived from the

[9] O. Corry, *Securitization and 'Riskification': Second-order Security and the Politics of Climate Change*, "Millenium: Journal of International Studies" 2012, Vol. 40, No. 2, pp. 235-258. See also: P. Polko, *Bezpieczeństwo w dyskursie politycznym RP (1989-2020)*, Warszawa 2022, pp. 43-57; P. Polko, K. Kujawa, *Constructing Security: Securitisation, Riskification and De+tion*, [in]: *Contemporary Understanding of Security and Its Contexts*, eds. P. Polko, B. Wiśniewski, Berlin 2024, pp. 25-42.

[10] J. Hagmann, M. Dunn Cavelty, *National Risk Registers: Security Scientism and the Propagation of Permanent Insecurity*, "Security Dialogue 2012, Vol. 43, No. 1, pp. 79-96.

[11] A. W. Neal, *Security as Politics: Beyond the State of Exception*, Edinburgh 2019, p. 248.

context in which it is embedded[12]. If so, then the goal for the students of security is to examine not only the said volatility and contextuality of security but also how the state authorities incorporate security politics, comprising various methods and procedures of managing and governing security issues, into the very core of the overarching state policy, to 'normalize it'.

Arguably, such normalization does not and should not be fathomed in terms of the stringent dichotomies proposed by the Copenhagen School, i.e. politicization vs securitization and securitization vs desecuritization[13]. Nor does it amount to what some champion as 'emancipation' from security perceived as a form of political oppression[14]. Instead, normalization of security means that the state's (governmental) security politics should amount to ordinary and mundane proceedings based on merit, not the logic of 'Othering[15]', distrust, resentment, exclusion, hostility, and conflict. In his book, Andrew W. Neal demonstrates the process of normalization of security politics based on the UK case and the profoundly political game between various British authorities, engaged in a tug-of-war aimed at making the strategy and politics of security more political and less dominated by the British government and secret services[16].

From the viewpoint of critical security studies, security and its policy are seen as suspicious and menacing because politicians often use them as the Foucaultian 'technology of power'[17]. Security then becomes constructed as a state of affairs in which the 'Other' (seen, inevitably, as the 'Enemy') posing a

---

[12] Ibid, pp. 50-67.

[13] O. Wæver, *Securitization and Desecuritization*, [in]: *On Security*, ed. R. Lipschutz, New York 1995, pp. 46-87.

[14] K. Booth, *Theory of World Security*, Cambridge 2007; C. Aradau, *Security and the democratic scene: desecuritization and emancipation*, "Journal of International Relations and Development" 2004, Vol. 7, pp. 388-413.

[15] It must be emphasized that for any identity (individual and collective alike) to come into existence there must also exist some *Other(s)*, against whom the identity of the former is created. According to Ted Hopf, "We cannot know what an identity is without relating it to another" (T. Hopf, *Social Construction of International Politics Identities and Foreign Policies, Moscow, 1955 and 1999*, New York 2002, s. 7.). This mechanism, being an intrinsic part of identity construction, is, in a sense, 'normal' and does not constitute a security Issue as such. However, this mechanism can escalate (or, more precisely, can be escalated) to become another, referred to as '*Othering*', in which those that do not belong to our group (social, ethnic, political, confessional, etc.) are discursively constructed as a threat (see e.g. Ch. Deacon, *Perpetual ontological crisis: national division, enduring anxieties and South Korea's discursive relationship with Japan*, "European Journal of International Relations" 2023, Vol. 29, No. 4, pp. 1041–1065; B. Çağatay Tekin, *Bordering through othering: On strategic ambiguity in the making of the EU-Turkey refugee deal*, "Political Geography" 2022, Vol. 98.).

[16] A. W. Neal, *Security as Politics…*

[17] M. Foucault, *Discipline and Punish: The Birth of the Prison*, New York 1977.

'threat' to 'Us' is always 'out there', according to the discourse deployed by the political elites, which use that narrative as the justification for sustaining conflictual policies that grant them power[18].

Andrew W Neal firmly opposes this perception of and approach to security and its policy. Upon examining the array of arguments laid out by authors who perceive security as 'anti-politics'[19], he concludes that what is needed to break away from the security vs politics dichotomy is to abandon the Hobbesian and Schmittean ontology and logic of security and replace it with the Machiavellian and Weberian ones[20]. Also, as mentioned before, he advocates an approach to security that accounts for its historical dynamics and contextual specificity. Such an approach is freed from and unconstrained by theoretical rigidity and dogmatism, which are said to be characteristics of the theory of securitization developed by the Copenhagen School, as pointed out not only by Neal, but also by numerous other scholars who are critical of the said theory. It is probably the combination of the elegant theoretical framework, a convincing line of argument in favour of 'politicization' of security, and a meticulous study of the complex process of evolution of 'problematization' of security (at the levels of security strategy and security politics) by the British political leaders and authorities that makes this volume genuinely illuminating, thought-provoking, and inspiring. Andrew W. Neal proves in his book that robust theories are essential for scholars to grasp the nature and meaning of social phenomena but it is even more important to ensure that those theories are as grounded in the social reality as the phenomena to be studied. And, last but not least, he reminds us that security, as one of the cardinal values that people strive to achieve, must be a subject of political choice and decision, just like the rest of those values.

BIBLIOGRAPHY:

1. Aradau C., *Security and the democratic scene: desecuritization and emancipation*, "Journal of International Relations and Development" 2004, Vol. 7, pp. 388-413.
2. Balzacq T., *Securitization Theory: How Security Problems Emerge and Dissolve*, London 2011.
3. Booth K., *Theory of World Security*, Cambridge 2007.

[18] D. Campbell, *Writing Security: United States Foreign Policy and the Politics of Identity*, Minneapolis 1998.

[19] A. W. Neal, *Security as Politics…*, op. cit., pp. 12-19.

[20] Ibid, pp. 19-28.

4. Broecker H., *Securitization as Hegemonic Discourse Formation: An Integrative Model*, Munich 2022.
5. Buzan B., *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Colchester 2016.
6. Buzan B., Wæver O., de Wilde J., *Security: A New Framework for Analysis*, Boulder 1998.
7. Çağatay Tekin B., *Bordering through othering: On strategic ambiguity in the making of the EU-Turkey refugee deal*, "Political Geography" 2022, Vol. 98.
8. Campbell D., *Writing Security: United States Foreign Policy and the Politics of Identity*, Minneapolis 1998.
9. Corry O., *Securitization and 'Riskification': Second-order Security and the Politics of Climate Change*, "Millenium: Journal of International Studies" 2012, Vol. 40, No. 2, pp. 235-258.
10. Deacon Ch., *Perpetual ontological crisis: national division, enduring anxieties and South Korea's discursive relationship with Japan*, "European Journal of International Relations" 2023, Vol. 29, No. 4, pp. 1041–1065;
11. Floyd R., *The Morality of Security: A Theory of Just Securitization*, Cambridge 2019.
12. Foucault M., *Discipline and Punish: The Birth of the Prison*, New York 1977.
13. Hagmann J., *(In-)Security and the Production of International Relations: The Politics of Securitization in Europe*, Abingdon 2014.
14. Hagmann J., Dunn Cavelty M., *National Risk Registers: Security Scientism and the Propagation of Permanent Insecurity*, "Security Dialogue 2012, Vol. 43, No. 1, pp. 79-96.
15. Hopf T., Social Construction of International Politics Identities and Foreign Policies, Moscow, 1955 and 1999, New York 2002.
16. Huysmans J., *The Politics of Insecurity: Fear, Migration and Asylum in the EU*, Abingdon 2004.
17. Neal Andrew W., *Security as Politics: Beyond the State of Exception*, Edinburgh 2019.
18. Polko P., Bezpieczeństwo w dyskursie politycznym RP (1989-2020), Warszawa 2022.
19. Polko P., Kujawa K., *Constructing Security: Securitisation, Riskification and Desecuritisation*, [in]: *Contemporary Understanding of Security and Its Contexts*, eds. P. Polko, B. Wiśniewski, Berlin 2024, pp. 25-42.
20. Stritzel H., *Security in Translation: Securitization Theory and the Localization of Threat*, Basingstoke 2014.

21. Wæver O., *Securitization and Desecuritization*, [in]: *On Security*, ed. R. Lipschutz, New York 1995, pp. 46-87.
22. Wolfers A., *"National Security" as an Ambiguous Symbol*, "Political Science Quarterly" 1952, Vol. 67, No. 4, pp. 481-502.

FOR AUTHORS

1. Submitted articles should not be published before and their quality will be put to the anonymous review.
2. The maximum volume of the article should not exceed 1.5 publishing sheet (60 thousand characters with spaces, approx. 30 typewritten pages). Languages of publication: Polish or English. It is necessary to attach a summary of the article in English (maximum 15 lines) together with separate keywords (maximum 5). Specific editorial requirements are presented below.
3. According to the guidelines of the Ministry of Science and Higher Education for scientific journals, the editors of "Ante Portas –Security Studies" require from the authors not only the reliability and accuracy of the merits, but also the compliance with ethical requirements relating to the publication of scientific papers. Therefore, information about all the people who contributed to the article in content, factual, financial or any other terms should be given. Hiding contribution to the creation of the publication is a reprehensible practice known as “ghostwriting”. In addition to a list of all the authors of the text, along with their workplace (affiliation) and information about the contribution of individuals in the creation of the article (who is the author of methods, concepts, principles, etc.), the information on the sources of funding of the publication (with number of grant), should be also included (in a footnote), together with the contribution of scientific research institutions, associations and other entities (ie. financial disclosure).

For more information please visit **www.anteportas.pl**

FOR REVIEWERS

1. Editors of "Ante Portas – Security Studies" make the initial verification of the submitted texts, comparing its subject with the journal's profile and confirming the compliance with editorial requirements.
2. The pre-approved text are forwarded for review to two persons mentioned in the list of reviewers cooperating with the publisher. In the case of a foreign language manuscript, at least one of the reviewers is affiliated with a foreign institution.
3. In the review process both the author and reviewers are anonymous (double-blind review process).
4. Reviewers evaluating the text fill in the Review Form. The Review Form is available on the journal's website.
5. The review has a consultative function, which means that the final decision regarding the acceptance of the text for printing is made by editors of "Ante Portas".
6. The detailed rules for reviewing of the articles conform to the guidelines of the Polish Ministry of Science and Higher Education.

For more information please visit **www.anteportas.pl**