UDK 355/359 CODEN SMOOAM ISSN 1409-8199

МЕЃУНАРОДНО НАУЧНО СПИСАНИЕ

СОВРЕМЕНА МАКЕДОНСКА ОДБРАНА

44

MINISTRY OF DEFENCE
REPUBLIC OF NORTH MACEDONIA

CONTEMPORARY MACEDONIAN DEFENCE

Vol. 23, Number 44, 2023

44

VOL. XXIII
SKOPJE
JUNE 2023

СОВРЕМЕНА МАКЕДОНСКА ОДБРАНА	Год.	Број	Стр.	Скопје
	23	44	1-122	2023
CONTEMPORARY MACEDONIAN DEFENCE	Vol.	No	pp	Skopje

СОВРЕМЕНА МАКЕДОНСКА ОДБРАНА

MINISTRY OF DEFENCE
REPUBLIC OF NORTH MACEDONIA

СОВРЕМЕНА МАКЕДОНСКА ОДБРАНА
CONTEMPORARY MACEDONIAN DEFENCE

ISSN 1409-8199
e-ISSN 1857-887X

Година 23, бр. 44, јуни 2023 / Vol. 23, No. 44, June 2023

Skopje
June 2023

MINISTRY OF DEFENCE
REPUBLIC OF NORTH MACEDONIA
CONTEMPORARY
MACEDONIAN
DEFENCE
Vol. 23, Number 44, 2023

EBSCO
HOST

СОВРЕМЕНА МАКЕДОНСКА ОДБРАНА

Издавач:
МИНИСТЕРСТВО ЗА ОДБРАНА НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
Министерство за одбрана
„СОВРЕМЕНА МАКЕДОНСКА ОДБРАНА“
„Орце Николов“ 116 1000 Скопје
Телефони: 02 3128 276, 02 3113 527
Интернет адреса:
WEB на Министерство за одбрана:
https://www.mod.gov.mk/современа-македонска-одбрана/
Списанието излегува два пати годишно.
ISSN 1409-8199
Скопје, Јуни 2023 година

CONTEMPORARY MACEDONIAN DEFENCE

Publisher:
MINISTRY OF DEFENCE OF THE REPUBLIC OF NORTH MACEDONIA

Ministry of Defence
„CONTEMPORARY MACEDONIAN DEFENCE“
„Orce Nikolov“ 116 1000 Skopje
Tel.: 02 3128 276, 02 3113 527
Internet address:
WEB of the Ministry of Defence:
https://www.mod.gov.mk/contemporary-macedonian-defense/
The magazine is published twice a year
ISSN 1409-8199
Skopje, June 2023

СОВРЕМЕНА МАКЕДОНСКА ОДБРАНА

МЕЃУНАРОДНО НАУЧНО СПИСАНИЕ НА
МИНИСТЕРСТВОТО ЗА ОДБРАНА НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Секретар: *Жанет* РИСТОСКА
Техничка подготовка: *Спиро* Јанев

CONTEMPORARY MACEDONIAN DEFENCE

INTERNATIONAL SCIENTIFIC JOURNAL OF
THE MINISTRY OF DEFENCE OF THE REPUBLIC OF NORTH MACEDONIA

Secretary: *Zhanet* RISTOSKA
Processing: *Spiro* JANEV
Proofreading and Editing: *Rozi* GROZDANOVSKA, *Martina* KIMOVSKA

CONTENTS:

Original scientific article
UDK 355.48:341.322.5(470+571:477)"2022/2023"
UDK 355.02:327(470+571:477)"2022/2023"

JUSTICE AT HEART OF THE WAR IN UKRAINE

Michel FOUCHER[1]
Antoine GARAPON[2]

Abstract: *Justice is definitely at the heart of the war in Ukraine. Crimes of all kinds have been accumulating there since 24 February 2022. They have the particularity of being both classic and unpublished; not that the new coexists with the old, but because they, on the contrary, are totally intertwined. Hence the need to differentiate between what is linked to the war itself and what is specific to this conflict. Distinguishing between the two not only provides benchmarks for present action, but also gives elements for understanding the future.*

Keywords: *War, Ukraine, justice, war crimes, Putin.*

An old crime in a new world

The Russian President bears full responsibility for the war of aggression against Ukraine under false pretexts. It is a deliberate choice and not a necessity attributable to NATO, a defensive alliance. But the crime of aggression, recognized as the one that makes all other war crimes possible, including crimes against humanity and genocide, is considered the "mother of all crimes" by the international judiciary community.

The old formulation of "crime against peace" gives all its meaning to the current situation: the Russian President then violated the "sacred value of treaties" to quote article 227 of the Treaty of Versailles, which expressly targeted the crime against peace. Let us not forget that the crime against peace was the first incrimination of a nation during the Nuremberg trials. Pacta sunt servanda ("The conventions must be respected"), and it should not be forgotten that the relationship between Ukraine and Russia was sealed by international treaties and the Budapest Memorandum (1994). It is therefore the founding crime against the international criminal law that was committed by Putin.

But, if the triggering of the "special operation" launched by the president of Russia targeted first and foremost Ukraine, the hostility of the discourse of the Kremlin has also been directed against the "collective West", especially Europe.

[1] Ph.D., French geographer, diplomate and essayist. A professor at ENS, IEP in Paris and the ENA.

[2] Ph.D, Institut des Hautes Etudes sur la Justice (IHEJ).

By the increase in the price of raw materials – which did not happen solely because of the afore-stated, but which he considerably increased lied – paired with the disinformation operations was intended to break the confidence of the public opinion in their governments. It is thus a direct attack on democracy, because this policy by definition aims at that countries in which there is a free opinion and elections. This crime against world order takes the form of an attack against democracies, by turning the mechanism of representation against himself.

Finally, this conflict deeply disrupted the energy markets and raw materials, so much so that almost all the countries of the world were practically affected by it. This profoundly destabilized the order of the world already shaken by the health crisis.

What is new is not aggression, but the state of the world – hence the interest of broadening the qualification of a crime against global peace and world order. Any war upsets the balance of the world, but it is not the same to destabilize the Westphalian order as to provoke a shock in a globalized world, that is to say, the world that is integrated and in which each one is dependent on the other. If the war of invasion is not new (perhaps even one of the oldest forms of warfare), the importance of the economy is quite unprecedented. Countries have reacted through the economy, among other things, the western countries responded by imposing sanctions aimed at isolating Russia. These sanctions are intended to strike, not directly, but through the economic system, by excluding a member of the world from the economic flows. Another novelty is the vote of the General Assembly of the Organization of the United Nations of 15 November 2022 deciding about the creation of a centralized register of damage, so as to facilitate the recovery after the cessation of fighting. There remains the difficulty of transforming the seized money into a special fund for the reparation of Ukraine, which is not self-evident from a legal point of view.[3]

The mechanism and the precautionary measures begin even during conflict. The time of action and the time of reflection on justice and reparation overlap. The issue of damages is addressed even before the conflict is over. The same goes for the justice whose court tries to settle before the end of hostilities. The idea is not new: the warnings of the Allies to the Axis powers during the Second World War that they would not only have to account for their crimes, but to make amends, were present since 1942.

What is new is the loop proposed and accepted between these offsets and the use of Russian assets. We observe the same phenomenon for evidence and the constitution of legal files already created. But, economics is not just a discipline or a sector of an activity, it is also a way of seeing the world. Putin benefited from the effect of surprise by brutally reintroducing politics into a world too economy oriented. He created a

[3] This can only go through only via an international treaty or internal laws, like the Canadian law of December 2022. Another strategy would be to return the seized assets so as not to incur the accusation of spoliation, but considering the Russian Federation as a pariah state (in the same way as Iran, for example) and therefore, for Western economies, to sanction the companies that would trade with it, so as to force it to sit down at the negotiating table to settle the question of war damage and reparation for serious attacks committed on civilian populations.

"drama" in a world that believed only in "trials"[4]; it made the event in a Europe which was hazed by the hypothesis of an "end of history", which neglected the passions and individual actions by focusing on the rational behaviours.[5] If comfort is the great enemy of freedom, the reduction to figures is that of politics.

If the war of 1914-1918 was an industrial war, the war of Ukraine adds the digital dimension to the industry, which continues to weigh. Digital provides new modes of making these decisive elements available for initiating proceedings. But, at the same time, it offers a plethora of evidence, as it was demonstrated with the Syrian example, thus there is a desire to centralize, keep, classify and make these decisive element for initiating a procedure, available. We now live, because of the economy and the digital, among others, in a fully integrated world. Unlike the Russians, who use the cyber weapon according to an old vision of the world, the Ukrainians have understood, since the beginning of the war, that digital is also a world.[6]

Putin only understood half of this new state of the world: he used interdependence as a weapon. As in Syria, he uses the ability of refugees to circulate as a weapon of mass destruction.[7] He relies on the anaesthetic power of comfort to push the Western opinions to capitulate, because they are too cold. He relies on the premium that accrues to barbaric behaviour in a gentrified world, to use the distinction of the late Pierre Hassner.[8] He leads a hybrid war, but in the service of a vision ancient: he continues to think in Westphalian terms in an interconnected world. Ukrainians are more modern: they have understood the world and play the opposite and area open.[9]

This war, like the pandemic, has already dealt a serious blow on globalization, like the First World War. But it is not going to make the Internet obsolete, any more than the wars of 20th century have stopped globalization. The challenge to democracies is however there. Among the answers they must find, justice occupies an important place.

War through crime

The Ukrainian war is both a regular war and an irregular war. It is regular, high-intensity, "classic" warfare, one could say, when only talking about asymmetrical conflicts, because it is carried out by armies and puts two sovereign States against each other who compare their strengths, with the terrain won and lost as their ultimate arbiter, conquered or lost. The modalities of the conflict are not unprecedented (think

[4]- Raymond Aron, Dimensions de la conscience historique [1961], préface de Perrine Simon-Nahum, Paris, Les Belles Lettres, 2011, p. 253.

[5]- Voir Datawar, « Bons chiffres, fausses prédictions ? Pourquoi la guerre en Ukraine a pris l'Europe par surprise » [en ligne], La Vie des idées, 25 octobre 2022

[6]The first cyberattacks against Ukrainian electrical installations took place on 23 December 2015.

[7]See the interview with Denys Chmyhal, Ukrainian Prime Minister: "Russia wants to create a tsunami of refugees, in order to destabilize European countries", Le Monde, 16 December 2022.

[8]Pierre Hassner, "The Barbarian and the Bourgeois", International Policy, no 84, summer 1999, p. 90-91.

[9]See Shi Zhan, "The First Metaverse War" [online], trans. by David Ownby, The Great Mainland, June 7, 2022

of the bombardment of Dresden) and no war is completely regular.[10] But, the irregular warfare directly targets civilians in their lives, i.e. by affecting their ability to survive.[11]

There is even a relationship between failures in regular warfare and irregular attacks against civilian infrastructure. Again, this is the oldest law of war which is flouted. Putin introduces, in the conduct of the war, a new category of crimes against humanity: a mixture of provocation (it is totally uninhibited and does not even take precautions to hide what he does), terror (he seeks less to break the enemy's morale than to terrorize it, as shown by his dangerous game with nuclear power at Zaporizhia) and inhumanity (by attacking hospitals and schools, even in undermining the cemeteries – everything happens as if, even more than the people, he wants to destroy the care for the sick and the children).

It is less the mass that interests him (a crime against humanity is an act committed within the framework of widespread or systematic attack) than what defines humanity as a common ground. He no longer seeks to dehumanize prisoners by mistreating them, by torturing them and raping them, and by killing what is human in them, but he wants to kill the sense of humanity of caregivers and educators by preventing them from doing their job. What is targeted by these crimes is civility, even civilization. Civilians are no longer collateral victims who are neglected and who bear the brunt of war, like soldiers or indiscriminate bombardments; they are now directly targeted to make them flee and to transform them into a weapon of mass destruction. The way of waging war has become more than barbarism.

This is why this "Putin war", which he has already practiced in Chechnya, in Syria and which he practices today in Ukraine, must speak to the conscience of humanity. The Ukrainian authorities - were not mistaken: they understood that it was necessary to fight on the ground on the front lines, but also, to wage war against crime perpetrated against civilians and against the sentiment of humanity, to investigate these crimes in such a way as to make justice possible. The entry into play of Wagner's men marks the coexistence of war by the army and a militia war.[12]

[10] On this subject, see Jean-Vincent Holeindre, La Ruse et la force. Another history of strategy, Paris, Perrin, 2017.

[11] The recent visit to Ukraine by Volker Türk, United Nations High Commissioner for Human Rights, made it possible to communicate to the UN, on 15 December 2022, information collected by his office on «summary executions and attacks on civilians» in more than a hundred villages and cities of Kyiv, Chernihiv and Sumy regions, between 24 February and 6 April 2022 (murder of 441 civilians). Mr. Türk, who noted that investigators were also trying to corroborate 198 other alleged murders, added that there were «strong indications» that summary executions described in the report of his Office could constitute the war crime of «intentional homicide».

[12] The recent visit to Ukraine by Volker Türk, United Nations High Commissioner for Human Rights, made it possible to communicate to the UN, on 15 December 2022, information collected by his office on «summary executions and attacks on civilians» in more than a hundred villages and cities of Kyiv, Chernihiv and Sumy regions, between 24 February and 6 April 2022 (murder of 441 civilians). Mr. Türk, who noted that investigators were also trying to corroborate 198 other alleged murders, added that there were «strong indications» that summary executions described in the report of his Office could constitute the war crime of «intentional homicide».

We could see a precedent in the use of private companies by Americans in Iraq, but these did not intervene directly alongside the regular fighters. At the very least, we are witnessing a de-formalization of war and a corresponding weakening of the law.

The bombardments (in particular with incendiary bombs, as recently in Kherson) are intended, not only to break the morale of the rear, but to scare them away and use the refugees as a weapon, like what the Russians did in Syria. There military strategy uses globalization and the ability of individuals to engage in mass migrations, which was less the case in the world of yesterday. But, the use of terror is not reserved for the enemy or to maintain order in his own troops. The filmed sanction of the man who deserted from Wagner is in this respect revealing of the "dual" character of the war (rather than hybrid, to reserve this adjective for spatialized warfare and despatialized).

A genealogical crime

There is a less spectacular part of the crimes committed during this war, which are not yet documented. This is especially the looting of the Kherson Museum and what can be likened to an erasure of Ukrainian culture. It is wrong that some have seen this as a "cultural weapon" used by Moscow. It is indeed the intention to deprive a people of access to its history. For Putin, there is no Ukrainian people. It is still too early to speak of cultural genocide,[13] but it is clear that the Russian elites do not tolerate the emancipation of a sovereign and independent Ukrainian nation, which would put an end to the dream empire of the Russian state.[14]

These facts take on a particular colour because of the history relations between the Russian authorities and Ukraine. All these crimes indeed resemble Stalinist crimes. We can't but recall Holodomor. Raphael Lemkin, the inventor of the notion of genocide, saw in this mass crime "the classic example of the Soviet genocide, the longest and most extensive experience of Russification: the destruction of the Ukrainian nation ".[15]

The crimes of the past shed light on the intentions of the perpetrators of the current war: the negation of the identity of a people. Regarding the deportation of children, we do not know much, except for the cynical statement that they were taken to Russia to receive "treatment appropriate to their condition". We got out of the propaganda

[13] In the statute of the International Criminal Court, it is a war crime. See the indictment of Ahmad al-Faqi al-Mahdi, a member of the Islamist extremist group Ansar Dine. Al-Faqi, who has pleaded guilty to war crimes charges related to the destruction of shrines and mausoleums Muslims in Timbuktu, was sentenced to nine years in prison.

[14] See Michel Foucher, "Ukraine-Russia, the mental map of the duel", Tracts Gallimard, no 39, May 2022; and Ukraine. A colonial war in Europe, Paris, L'Aube, 2022.

[15] Raphael Lemkin, "The Soviet Genocide in Ukraine" [1953], Commentary, vol. 127, No. 3, 2009, p. 637-652. See also Yves Cohen, Jean-Marc Dreyfus, Luba Jurgenson and Pierre Raiman, " L'écho du Holodomor" [online], Spirit, November 2022.

to enter into the totalitarian language with its "insolence of lies". This practice had already been used in Crimea.[16]

Russian law makes these children adoptable in just one day. It is based on facts substantial to complaint that was filed on 21 December 2022 before the International Criminal Court for genocide.[17]

How can one not connect this with the deportation of approximately 200 000 Polish children by the Germans during the Second World War for the "Germanization"? We know that some of these children were destined for adoption, which is reminiscent of the practices of dictatorships in South America or the Francoism.

Using children means amputating the victimized group's capacity for perpetuation. Whether it's culture or children, Russia is indulging in Ukraine to a genealogical crime, by showing their will to deprive a people of cultural ancestry or biological descent. These possible crimes must be investigated or, failing to be able to conduct this, a collection of as much information as possible about them needs to be substantiated for the purpose of filing charges. Ukraine assumed this work of justice since the beginning of the war, with the democracies which have become aware of the seriousness of the facts: common and mobile teams intervene from the beginning of hostilities, so as to introduce justice as soon as possible and as adequate as possible. Showing unprecedented confidence in the truth of from the belligerent.

The urgency of a judicial response

Faced with this crime of aggression and this war through crimes, a response is required from the judiciary. The idea of convening an ad hoc tribunal was very quickly launched by Philip Sands.[18] Several approaches to international justice are ongoing, official[19] or citizen initiative.[20]

Three possibilities are available today: go through the International Criminal Court, create a tribunal under the aegis of the UN, like the International Criminal Tribunals for

[16] In Crimea, there were two waves of deportation of the Tatar population, under the Russian Empire and under the Soviet regime (in the 1940s). Men, women and children were sent to Central Asia, especially in Uzbekistan. It is therefore a practice well inscribed in the culture of Russian leaders.

[17] The complaint, filed by the association Their Freedom is Ours, represented by Me Emmanuel Daoud, on the deportation of 13,000 children

[18] Philippe Sands, "Putin's use of military force is a crime of aggression", Financial Times, February 28 2022

[19] Sergiy Kyslytsya, Ambassador of Ukraine to the United Nations, and Christian Wenaweser, the envoy of Liechtenstein, proposed the drafting of a draft resolution establishing a tribunal international court to prosecute Russia's top leaders for crimes of aggression against Ukraine. Given the right of veto of the Russian Federation in the Security Council, a recourse to the General Assembly is the only way possible.

[20] A declaration of March 4, 2022, adopted by high-level politicians and international jurists. nationals, refers to the precedents of Nuremberg and Tokyo to affirm that the «special tribunal should be constituted according to the same principles which guided the Allies in 1942" and that it could be «set up quickly». The signatories proposed a "Declaration on a special tribunal for Punishment for the Crime of Aggression against Ukraine", intended to be signed by the governments

the former Yugoslavia and Rwanda, or support the tribunal on the Council of Europe. Almost insurmountable obstacles close the first two opportunities; what remains is the European way, which seems both the most practicable and the most significant.

What remains are the legal obstacles that should not lead to renouncing any judgment of the rulers of the Russian Federation. And it is a political question, more than a legal one.

History teaches us since 1945 that there is no security in Europe without an individual sanction – which goes through trials like those in Nuremberg or Tokyo – authors aggressions, without critical examination of the past by elites and parties, teachers and clergy, and the installation of democratic regimes and the rule of law, all of which are the foundations of true reconciliation. Russia will become frequented again when the Memorial association has regained their right of establishment and public pedagogy.

Putin keeps referring to the "Great Patriotic War" but, once again, he has not learnt all the lessons. He does not expand his look at the beginnings of the Second World War, which began with the German-Soviet pact, no more than the world has discovered at the end of this war: the Shoah.

He therefore did not understand the dimension re-founder of this crime in the construction of Europe. He definitively prevented from doing this work by banning Memorial. This interdiction is indicative of a desire to undermine any prospect of justice on the gulag. Historical justice has still not penetrated the culture of Russian elites, unlike the people who keep the memory alive in their beings, as the work on the Memorial has shown.

"Those who do not know their past are doomed to relive it", it is often said. This is demonstrated by today's Russia, which has locked itself into an increasingly deadly (and outdated) pride. Isn't it one of the great lessons of the 20th century that peace was not the ultimate act of war, but that it had to share this eminent place with justice? Every war in this century has ended with an intensified desire for justice.[21] Justice is the condition for lasting peace and stability in Europe.

REFERENCES:

-Convention de Genève (I) sur les blessés et malades des forces armées sur terre, 1949

-Convention de Genève (II) sur les blessés, malades et naufragés des forces armées sur mer, 1949

-Convention de Genève (III) sur les prisonniers de guerre, 1949États parties et signataires

-Convention de Genève (IV) sur les personnes civiles, 1949États parties et signataires

[21] See Articles 227 and 228 of the Treaty of Versailles, then Nuremberg and Tokyo, then the International Criminal Courts (Rwanda, ex-Yugoslavia), then the Treaty of Rome and the International Criminal Court. In all these cases, allied to justice, it is a new system of collective security that came out: the League of Nations after the First World War, the United Nations after the Second, the system of complementarity with the International Criminal Court, which was part to globalization after the 1990s, which is now collapsing before our eyes. Our task of tomorrow will be to build a more appropriate justice and to tackle a new collective security system.

-Protocole additionnel (I) aux Conventions de Genève, 1977

-Protocole additionnel (I) aux Conventions de Genève, 1993

-Protocole additionnel (I) aux Conventions de Genève, 2005

-MAURO Frédéric, « Guerre en Ukraine : quels enjeux pour le droit international ? », *Revue Défense Nationale,* 2023/2 (N° 857), p. 43-55. DOI : 10.3917/rdna.857.0043. URL : https://www.cairn.info/revue-defence-nationale-2023-2-page-43.htm

-Camille Marquis-Bissonnette - Guerre en Ukraine et droit international, un face-à-face complexe, 24 février 2023 Paris: Idées -https://www.ledevoir.com/opinion/idees/783004/idees-guerre-en-ukraine-et-droit-international-un-face-a-face-complexe

Original scientific article
UDK 355.45:005.334(497.16)
UDK 355.02(497.16)

FROM THE PROTECTION OF CRITICAL INFRASTRUCTURE TO THE RESILIENCE OF CRITICAL ENTITIES IN MONTENEGRO

Dražen BOŽOVIĆ[1]

Abstract: *Shifting the center of gravity of modern threats from military to a wide range of non-military threats on the one hand, and the rapid technological development on the other hand, has turned modern society into a technologically dependent society that makes it more vulnerable to various technological accidents, natural disasters, criminal activities, terrorism and various other forms of asymmetric threats, where maintaining the functioning of the system of vital facilities and services (critical infrastructure), becomes one of the priority security challenges of modern society.*

In this sense, the EU adopted numerous documents in this area in the first decade of the 21st century, the most significant of which are Directive 114/2008 on the identification and marking of European critical infrastructure and assessments that should improve protection with the aim of encouraging and harmonizing national efforts for critical infrastructure protection (CIP). More and more frequent and diverse crises in the first decade of its implementation indicated the limitation of this concept, which was aimed at the protection of infrastructure facilities. In this sense, the EU conducted an evaluation of the CIP concept, which resulted in the introduction of the new Directive (EU) 2022/2557 for the resilience of critical entities, which replaced Directive 114/2008.

This paper deals with the analysis of relevant documents for strengthening the resilience of critical entities, and above all Directive (EU) 2022/2557 for strengthening the resilience of critical entities and its implementation in the national security systems of Montenegro. The conducted research points to the urgency of developing the concept of critical entities of resilience (CER) on the national level, and within the same concept of business continuity - the functioning of the economy and social entities in crisis situations. At the end of the paper, a possible model of the process of implementing the CER concept into the existing security system of Montenegro was proposed, which also needs to be reorganized in accordance with modern needs. The model includes planned, organized and time-aligned activities for the preparation of numerous conceptual and normative legal documents.

Key words: *critical infrastructure, critical subject, resilience, business continuity, crisis management.*

Introduction

Until the end of the 20th century, the defense system was the basis of national security and all actions and procedures were subordinated to it. Over time, the range of threats expanded and threats, such as terrorism, cyber-attacks, natural disasters, technical and technological and other disasters, became more and more prominent, which due to complex interdependence gain a multiplicative effect. Accordingly, the concept of security began to be reshaped

[1] Humanistic Studies, University of Donja Gorica, Podgorica, Montenegro

since the end of the Cold War, and reached its culmination after the terrorist attacks on New York, Madrid, London, disasters in the form of typhoons, earthquakes, tsunamis, as well as various accidents, which increasingly affected economies, infrastructure and population. As a result of these events, concepts such as risk management, emergency management, crisis management, protection of critical infrastructure and others are coming to the center of the security discourse. Apparently, these terms represent new functions in the security system. However, most of them have existed before in the function of the defense system, but by shifting the center of gravity from military defense to national security, they come to the fore and take on a new form.

One of the increasingly prevalent security discourses is the critical infrastructure, which consists of facilities, products and services, the destruction or cessation of which would have significant consequences on the lives of the citizens and the country's security situation. Taking into account the changed forms of danger and the consequences for citizens, property and general security, the protection of critical infrastructure occupies an increasingly important place at the national and international level (UN, OECD, NATO, etc.). Driven by the experiences of terrorist attacks, in 2004 the EU initiated the procedure of adopting a comprehensive strategy for the protection of critical infrastructure, which resulted in the adoption of the European Program for Critical Infrastructure Protection (EPCIP) and Directive (EC) 114/2008 on the identification and marking of European critical infrastructure and assessments that should improve protection.

However, before the concept of critical infrastructure protection could fully come to life, the COVID-19 pandemic and the war in Ukraine highlighted its weaknesses. The EU therefore conducted an evaluation of the CIP concept, which pointed to the limitations of the CIP concept and the need to expand it, from protection to resilience and from infrastructure to subjects. The result is the adoption of the new Directive (EU) 2022/2557 for the resilience of critical entities, which replaces Directive 114/2008.

As a candidate for EU membership, Montenegro has the obligation to harmonize the national legislation with this directive. With the adoption of the Law on CIP in 2019, the process of establishing the CIP system in Montenegro began. Sharing the fate of the region in which Montenegro is located, it faced the weaknesses of the CIP concept and the need to improve and expand it even before the adoption of the critical entities resilience (CER) Directive. Taking this into account, the question arises as to whether the establishment of a system of resilience of critical subjects should be viewed as an obligation from the EU accession process or as a priority as a national need to strengthen resilience given the frequency and intensification of various disturbances and threats.

Practice shows that new functions, when implemented in a planned and organized manner, make sense and enrich the existing security system. However, if these changes are not meaningful, planned and in accordance with the wider social context, they can cause confusion and dysfunction of the security system.

In this sense, the subject of research in this paper is the way to move from the concept of CEP to the concept of resilience of critical subjects. The goal is to consider which contents should be introduced and in what way, in order to establish a new concept of resilience of critical subjects. Content analysis, historical and comparative methods were applied in the work. The paper is divided into four parts: evolution of the concept of resilience of critical entities, EU concept of resilience of critical entities, evaluation of the concept of CIP in Montenegro and, finally, a possible model of the development process of the system of resilience of critical entities.

Evolution of the concept of resilience of critical entities

The term critical infrastructure protection (CIP) began to appear in the eighties of the last century as a point of reference for the creators of public policy and security, due to the increasing risk and vulnerability of large infrastructure systems, the cessation of regular functioning of which would have major consequences for the functioning of society and the economy. The term "critical infrastructure" is becoming more and more present in contemporary practice and theory with the increase in the danger of asymmetric threats, especially terrorism. Accordingly, after the terrorist attacks of September 2001, critical infrastructure has become an important and essential part of national security, and its protection is one of the priorities of every state.

Thus, after the terrorist attack on the federal building in Oklahoma City in 1995, the President of the United States of America (USA) used the phrase Critical Infrastructure Protection (CIP), then the Commission for Critical Infrastructure was formed, which in 1996 defined the CIP Policy, followed by numerous strategies and plans dealing with CIP. "CI and basic resources is a term that refers to a wide range of different assets and properties that are necessary for the daily functioning of the social, economic, political, and cultural systems in the United States." Any interruption in the elements of CI poses a serious threat to the proper functioning of these systems and can lead to property damage, human casualties and significant economic losses." (Murray, T.G.: 2012:31).

Other countries (United Kingdom (UK), Australia, Canada, etc.) have devoted themselves to CIP by creating national strategies and plans (see Figure 1). For Australia, "CI represents those physical facilities, supply chains, information technology and communications networks, which, if destroyed or permanently disabled, could significantly affect the nation's social or economic well-being, or affect Australia's ability to maintain its national defense and ensure national security", which shows that CI also includes supply chains and information technology.

Faced with the increasing danger of terrorist attacks, the EU has a more serious attitude towards CIP and in 2004 the European Council asked the European Commission to prepare a comprehensive strategy for the protection of critical infrastructure. Already in 2005, the EC adopted the European Critical Infrastructure Protection Program (EPCIP), and the key pillar of this program is Directive (EC) no. 114/2008 adopted on 8 December 2008 on the identification and marking of European critical infrastructure and assessments that should improve protection. After that, for the next ten years, the EU adopted numerous documents, which deal with CEP from various aspects, and which member countries and candidates should implement. For the EU, "CI is an asset, system or part of it that is located on the territory of a member state and that is necessary for the maintenance of key social functions, health, safety, security, economic or social well-being, and the disruption or destruction of which would have a significant impact to the member country." (Article 2a: Directive 2008/114).

At the same time, faced with numerous new challenges, risks and threats, the Organization of the United Nations (UN), The Organization for Economic Co-operation and Development (OECD) for the purpose of Disaster Risk Reduction (DRR) aims to develop a resilient society, especially resilience and security of the critical infrastructure.

The term resilience is used to describe the stability of the system and its ability to absorb changes and disturbances was first used by Holing in 1973 (Holing, C, S: 1973: 1-23). The English word resilience comes from the Latin verb resilire, which means jumping back or recovering (Pavićević: 2016). In recent years, the concept of resilience has become one of the most important concepts with central importance for disaster risk reduction and community resilience to resist the negative impacts of disasters at the local, national and global levels.

According to the International Strategy for Disaster Risk Reduction, since 2009, resilience is the ability of a system, community or society exposed to hazards to resist, absorb, respond to the consequences of hazards in a timely and effective manner, and recover from them, including the preservation and restoration of its essential basic structures and functions (ISDR: 2009). Building resilience takes center stage in the Hyogo Framework for Action 2005-2015 (HFA) and the Sendai Framework for DRR 2015-2030, which constitute key guidelines in the field of disaster risk reduction. This contributes to progress towards the achievement of the Millennium Development Goals, among which is the significant reduction of damage from disasters to critical infrastructure and the disruption of the provision of basic services, especially when it comes to health and educational institutions, through the development of their resilience by 2030.

OECD, dealing with "Critical Risks" and their disruptive consequences, in the Recommendation of the Council on the Governance of Critical Risks recommends a combination of protective measures and non-structural measures to reduce critical risks through: strategic planning to build safer and more sustainable communities. It also recommends the development of fiscal and regulatory options to promote spare capacity, diversification or backup systems to reduce the risk of failure and extended periods of disruption in critical infrastructure systems. Encouraging businesses to take steps to ensure business continuity is recommended, with a particular focus on critical infrastructure operators, namely:

1) by developing standards and tools designed for risk management for businesses or provision of basic services;
2) by ensuring that critical infrastructure, information systems and networks continue to function after a shock;
3) requiring emergency services located in CI facilities to maintain plans to ensure that they can continue to perform their functions in the event of an emergency to the extent practicable;
4) encouraging small businesses in the community to undertake proportional business resilience measures.

The OECD Recommendation on the Governance of Critical Risks (2014) acknowledges the importance of critical infrastructure resilience and security as a key element of national resilience.

After a wider debate conducted in 2006 in the USA on the approach to CIP, excessive focus of state policies on the CIP from terrorist attacks, while neglecting other threats, was noted. Shortly thereafter, the term "resilience" entered official American documents. The National Security Strategy prioritized the concept of resilience over the older concept of prevention and linked the "structural resilience" of critical infrastructure to the "operational resilience" of emergency services, government institutions and private companies in crisis. The UK National Security Strategy (2010), embraced resilience as a risk management strategy suitable for dealing with unpredictable risks. The Defense and Security Strategic Review (2010: 2015) defined tasks including the security and resilience of infrastructure most critical to sustaining the nation (including nuclear facilities) from attack, damage or destruction. Also, the establishment of a Council for Security and Resilience of Infrastructure was defined, which would significantly improve the cooperation between the public and private sectors, because: "The resilience of the UK depends on all of us - emergency services, local and central government, businesses, communities and individual members of the public". The following defense and security strategic documents without exception include critical infrastructure resilience among the pillars of national security. Australia has had an institutionalized approach to critical infrastructure resilience for nearly two decades, with the adoption of the CER Strategy, the Critical Infrastructure Security Act and other documents.

In accordance with the security environment, NATO decided to improve resilience (Warsaw Summit, 2019), and for the first time emphasis was placed on the joint strengthening of the concept of resilience, critical infrastructure, energy and communications (point 6, London Declaration, 2019) and started preparations for the adaptation of NATO until 2030, which are primarily reflected in increasing the resilience of the alliance and its members, by emphasizing that resilience remains a national responsibility, but that a more integrated and better coordinated approach has been adopted, all with the aim of reducing vulnerability and ensuring functioning of the system in conditions of peace, crisis and conflict (Strengthened Resilience Commitment 2021).

Faced with new forms of disruption, the EU in 2019 began an evaluation of the concept of Critical Infrastructure Protection, which resulted in the proposal of a new Directive for the resilience of critical entities.

It can be concluded that the idea of continuity of functioning of the economy and society during various crises and disturbances had its evolution depending on the demand, so it can be divided into 4 phases: physical protection of CI after terrorist attacks; transition to treatment of other hazards and protection of services; and then moving on to the concept of resilience, in order to finally move on to the resilience of subjects.

However, consideration of this problem requires taking into account some connections, which were represented in some other circumstances. Thus, the Finnish National Emergency Supply Agency (NESA) on its website proudly highlights its hundred-year tradition, which it divides into three phases:

- The first phase (1924-1955), Establishment and operation of the National Wartime Economy Committee, which includes several forms of organization.
- The second phase (1945-1992), The period of total national defense.
- Third phase - The period of systems, 1993 The National Emergency Supply Agency (NESA) started operations.

As can be seen in the first two phases of development, this system was in the function of military defense. Today, however, the focus of supply operations security is increasingly shifting towards ensuring the operational capability of critical infrastructure in the event of various emergency situations. In accordance with the abovementioned, in Finland they do not consider the resistance of critical subjects as a novelty. The need to develop national approaches to CER is emphasized, because countries are so different that there is no way that one model fits all countries, so the essence is only to harmonize the national approach with the EU's CER approach.

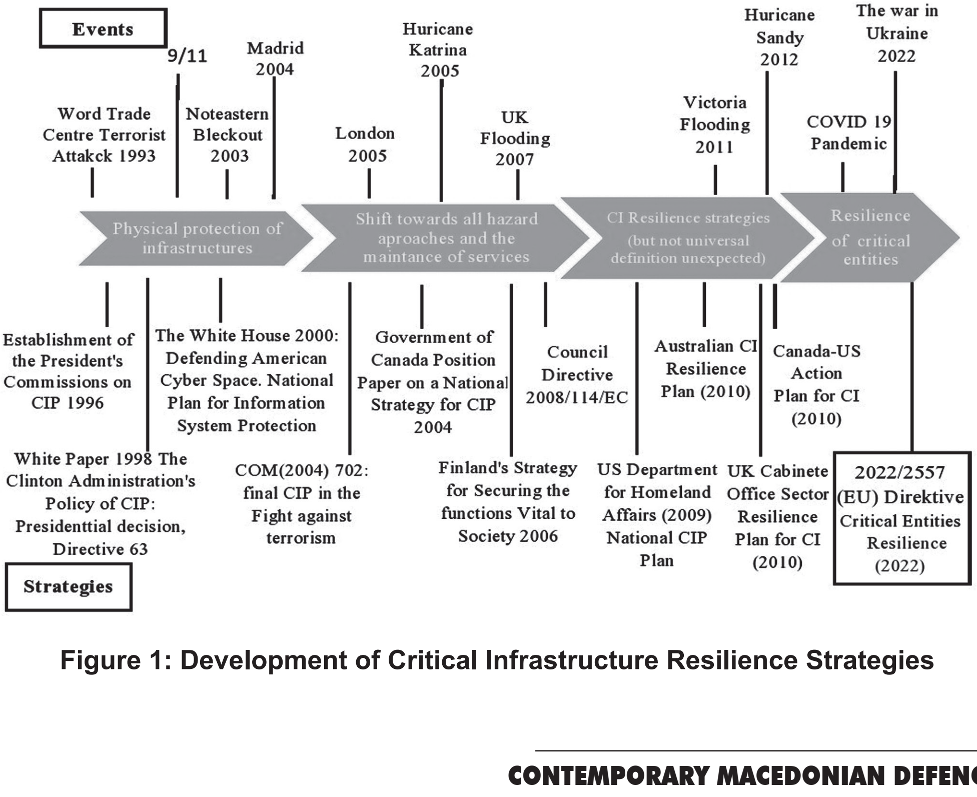

Events
Word Trade Centre Terrorist Attakck 1993
9/11
Noteastern Bleckout 2003
Madrid 2004
London 2005
Huricane Katrina 2005
UK Flooding 2007
Victoria Flooding 2011
Huricane Sandy 2012
COVID 19 Pandemic
The war in Ukraine 2022
Physical protection of infrastructures
Shift towards all hazard aproaches and the maintance of services
CI Resilience strategies (but not universal definition unexpected)
Resilience of critical entities
Establishment of the President's Commissions on CIP 1996
White Paper 1998 The Clinton Administration's Policy of CIP: Presidenttial decision, Directive 63
The White House 2000: Defending American Cyber Space. National Plan for Information System Protection
COM(2004) 702: final CIP in the Fight against terrorism
Government of Canada Position Paper on a National Strategy for CIP 2004
Finland's Strategy for Securing the functions Vital to Society 2006
Council Directive 2008/114/EC
US Department for Homeland Affairs (2009) National CIP Plan
Australian CI Resilience Plan (2010)
UK Cabinete Office Sector Resilience Plan for CI (2010)
Canada-US Action Plan for CI (2010)
2022/2557 (EU) Direktive Critical Entities Resilience (2022)
Strategies

Figure 1: Development of Critical Infrastructure Resilience Strategies

It is also important to point out that in the second half of the 20th century in the former SFRY, within the framework of the system of General National Defense and Social Self-Defense (ONO & DSZ), the concept of the functioning of the economy and social activities during war existed in practice. In the changed circumstances, a similar system exists in these areas even today, on a limited scale, for the holders of defense preparations who plan to provide facilities, products and services of special importance for the defense (Article 17, Law on Defense: 2/2017). However, it can be said that a comprehensive modern concept of business continuity, which would serve to strengthen the integrity of critical entities, has not been developed.

European Union's Concept of Critical Entities Resistance

As already mentioned, the EU established the concept of CIP through the EP CIP, Directive 114/2008, and other documents. Regarding the EU CIP, the initial basis in the mentioned documents are the benchmarks for determining and labeling ECI and assessments that should improve protection, which is also given in the very name of the Directive. The need to establish a line of communication and determine contact persons at all levels, from the operator through the sector and national level to the EU, was also defined. Cross-sector benchmarks for determining potential ECIs have been defined:

a) Number of victims (possible number of dead and wounded);
b) Consequences for the economy (which are assessed with regard to the economic importance of losses and/or knowledge of the quality of products and services, including possible impacts on the environment)
c) Impact on the public (assessed in terms of impact on public confidence, physical suffering and disruption of daily life; including loss of essential services).

The COVID-19 pandemic, the war in Ukraine and other circumstances cast doubt on the relevance and effectiveness of the Directive, so in 2019 the EU began its evaluation, which established that the security environment has changed significantly since the Directive entered into force. It became obvious that measures related only to individual assets are not sufficient to prevent the occurrence of all disturbances, so on 14 December 2022, Directive 2022/2557 on the resilience of critical entities and on the repeal of Directive 2008/114/EC was adopted. Instead of protecting a limited set of physical infrastructures whose disruption or destruction would have significant cross-border effects, the objective of the CER Directive is to increase the resilience of entities in the member states that are critical for the provision of services key to the maintenance of vital social functions or economic activities in the internal market in numerous sectors on which the functioning of many other sectors of the Union economy is based (Directive (EU) 2022/2557). In addition, by taking measures to increase the resilience of critical entities, the probability of disruptions/incidents that cause work interruptions and negatively affect the provision of key services in certain member states and throughout Europe will be reduced.

On the same day, the EU adopted Directive (EU) 2022/2555 on measures for a high common level of cyber security throughout the Union, amending Regulation (EU) no. 910/ 2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Considering that the NIS 2 Directive introduces comprehensive requirements for a large number of entities in order to ensure their cyber security, the issues covered by it are exempted from the scope of the new CER Directive. The new approach will consist of a combination of binding and non-binding measures and should ensure a stronger link between measures to increase cyber resilience and other types of resilience. Member States have 21 months to transpose both Directives into national law. During that time, the member states adopt and publish the measures necessary to comply with them.

In order to ensure a comprehensive approach to the resilience of critical entities, each member state should have done a risk assessment and adopted a strategy for strengthening the resilience of critical entities by 17 January 2026. The risk assessment should include all relevant natural and man-made risks that may affect the provision of key services, including accidents, natural disasters, public health emergencies such as pandemics, and hostile threats, including criminal acts of terrorism. When carrying out those risk assessments, Member States should take into account other general or sectoral risk assessments carried out in accordance with other acts of Union law. Member States are encouraged in particular to develop guidelines and methodologies, support the organization of exercises to test their resilience and ensure the training of personnel of critical subjects.

Within three years after the entry into force of the new Directive, each member state adopts a strategy to strengthen the resilience of critical entities, which contains at least the following elements:

a) strategic goals and priorities, taking into account cross-border and intersectoral interdependencies;
b) management framework for achieving strategic goals and priorities, including a description of the roles and responsibilities of various bodies, critical subjects and other parties involved in the implementation of the strategy;
c) measures to strengthen the general resilience of critical entities, including a description of the risk assessment;
d) the procedure used to determine critical subjects;
e) procedure supporting critical entities, including measures to improve cooperation;
f) main bodies and relevant participants, that are not critical subjects, and that are involved in the implementation of the strategy;
g) policy framework for coordination between competent authorities and performing supervisory tasks;
h) description of the measures already established, the aim of which is to

facilitate the implementation of the obligations of the Directive to small and medium-sized enterprises in the sense that the relevant Member State has determined as critical entities.

The following elements of resilience of critical subjects can be distinguished from the Directive: risk assessment for critical subjects; technical and organizational measures; developing a resilience plan; eligibility verification and incident reporting.

Member States shall ensure that critical entities take appropriate and proportionate technical and organizational measures to ensure their resilience, including measures necessary to:

a) preventing the occurrence of incidents, among others by means of measures to reduce the risk of disasters and measures to adapt to climate change;
b) appropriate physical protection of sensitive areas, facilities and other infrastructure, including fences, partitions, tools and routine procedures for monitoring the area, as well as equipment for detection and access control;
c) resisting the consequences of incidents and mitigating such consequences, including the implementation of procedures and protocols for managing risks and crisis situations and routine warning procedures;
d) recovery from accidents, including measures for business continuity and determination of alternative supply chains;
e) ensuring appropriate management of employee security, among others by determining the categories of personnel performing critical functions, determining the right to access sensitive areas, facilities and other infrastructure, as well as sensitive information and determining special categories of personnel with regard to Article 12;
f) informing the relevant staff about the measures mentioned in points (a) to (e).

Member States should ensure that critical entities establish a resilience plan detailing the aforementioned measures. Considering that all the mentioned documents that deal with strengthening the resilience of critical entities enhance the functioning of the economy and society, it is necessary to explain business continuity management in more detail, considering that it represents a newer concept. Since resilience is considered the ability for the organization to continue functioning even in the most difficult conditions, there are cases where it is identified with business continuity. However, resilience and business continuity cannot be considered synonymous. Resilience is a broader concept and includes the management of risks, continuity, security and crisis situations.

The modern concept of Business Continuity Management Systems (BMCS) has recently been regulated by the standards ISO 22 300 and ISO 22 301, which can generally be applied to organizations of any type and size. ISO 22301: 2012 defines business continuity as the ability of an organization to continue delivering products or services according to an acceptable pre-defined volume after the occurrence of a disruption that disrupts the organization's regular business operations (Introduction to

Business Continuity). This standard requires the development of a Business Continuity Policy, which determines the direction and generally defines what is to be achieved, and determines who is responsible for what, because the management should ensure that the business continuity management system is compatible with the strategic direction of the organization. Then the Business Continuity Strategy has been developed, which includes the assessment of requirements for the recovery of interrupted key business processes, the identification of options for the recovery of key business processes and the selection of the most cost-effective possible solutions. Finally, the Continuity Plan is the most important document, which consists of several documents for solving specific problems, containing: a) purpose, subject and area of application and goals; b) roles and responsibilities of the team that will implement the plan; c) measures for applying the decision; d) criteria for activating the plan; e) internal and external interdependencies; f) required resources; g) reporting requirements; process for revocation/termination (ISO 22 301:2012).

The basis for the development of the Strategy and the Business Continuity Plan (BCP) is analysis because it identifies what to focus on, which are the most important processes in the organization, and consists of: Business Impact Analysis (BIA) and Risk Analysis. A risk assessment identifies potential hazards such as weather, earthquake, fire, supplier failure, utility outage, or cyber-attack, and assesses areas of vulnerability in the event of a hazard. On the other hand, BIA is an ongoing process that determines and assesses the potential effects of interruptions on critical business operations as a result of some form of accident or emergency. At its core, it includes a research component that reveals all vulnerabilities, and a planning component for developing strategies to minimize risk and can serve as a starting point for a recovery strategy from an extraordinary event, and the resources and materials needed to continue regular business.

Evaluation of the concept of critical infrastructure protection in Montenegro

In 2019, Montenegro adopted the Law on Designation and the Critical Infrastructure Protection (Zakon o ZKI, 72/19), which implemented Directive (EU) 2008/14 into Montenegrin legislation. After that, the Department for coordination and supervision in the field of critical infrastructure was established, the responsibilities of which are the following: performing inspection supervision in the area of critical infrastructure and control of work through the implementation of the Law, coordination of the work of all coordinators in operators of critical infrastructure at the local and state level, implementation of measures to eliminate the consequences in case of threats in all forms of objects of critical infrastructure, training of coordinators of critical infrastructure, implementation of preventive activities for the purpose of CEP, establishment of international cooperation and exchange of data with institutions dealing with CEP.

Furthermore, in 2021, the Regulation on the determination of sectoral criteria and the Rulebook on the detailed content of the security plan for CIP were adopted, which were marked with the appropriate level of secrecy in accordance with the Law regulating data secrecy. Although in Montenegro the concept of CIP has not yet taken root in practice, several events in the last two years have clearly pointed out the weaknesses of the concept of CIP and the need to move to the concept of the critical entities resilience (CER). In accordance with the training program, in 2021, the Police Academy organized a training for lecturers in the field of CIP for about 15 participants. At a number of CI operators, persons responsible for CI have been appointed and for them already in 2021, the first training and certification by the Montenegrin Center for Training and Education of Adults was organized. However, no security plan has yet been prepared, although the Methodology for the preparation of these plans has been prepared and adopted in accordance with the Law (alternative options are being used: plans for the physical and technical protection of facilities, protection and rescue plans, etc.). On the basis of the Regulation on the determination of sectoral criteria, the Ministry of Internal Affairs sent letters to all ministries to determine within the legal term of 6 months the facilities and other infrastructure that, in accordance with the Law and Regulation, belong to the category of critical infrastructure.

Like many other countries, Montenegro has repeatedly been the target of cyber-attacks, but the multi-day attack started on 22 August 2022, on government servers and key infrastructure, which disabled access to their websites and emails, was the largest in scope and caused the most damage. The energy sector and finance were the most affected. The state responded to the decline of the tax system by introducing the so-called offline mode of operation. As the state's power system was under threat of a cyber-attack, ''Elektroprivreda" temporarily stopped providing part of its services and switched to the so-called manual mode of operation with the aim of minimizing damage. Montenegro's Euro-Atlantic partners were involved in repairing the consequences. To prevent future attacks, the country has updated its cyberspace protection protocol, suggesting to citizens to use only licensed operating systems and to back up their essential data.

The COVID-19 pandemic caused disruptions in the functioning of economic and social entities in the provision of basic services. The disruption affected all economic sectors, including tourism, which accounts for about 24% of Montenegro's GDP, which was the most affected. At the first moment of the pandemic, there was a threat of disrupting the food supply chain with basic food items, however, this problem was overcome with the stabilization of regional and global markets. The disruption had the greatest impact on the health and education system, which required adjustments on the fly. Modern information technology has made it possible to switch the education system to online teaching very quickly. In the health system, the problems were reflected in the deficit of medical equipment and materials for this form and scope of the pandemic, but above all in the lack of plans and standard operating procedures for handling such emergency situations.

The next disruption - the global crisis due to the war in Ukraine confirmed the problem of supplying energy and consumer goods. The problem of supplying basic food items came to the fore again, primarily due to the unjustified underdevelopment of the food sector and the abolition of state commodity reserves, which could have buffered such disruptions. Due to the lack of basic food products and energy sources, Montenegro was forced to buy deficit goods at unfavorable prices in unfavorable circumstances.

It was shown that the CIP system, which aimed to ensure the uninterrupted functioning of basic infrastructures, was not preemptively prepared for these types of disruptions. The fortunate circumstance was that the small system could be more easily adapted to the circumstances and solve problems (procurement of food and other consumer goods, medical supplies, provision of health and educational services, etc.). However, the disruptions left big consequences in this case on the country's economy, but if resilience has not strengthened, the question is what will be the consequences of the next disruption.

Experiences of crises from the recent past in Montenegro have brought to the forth the discussion on the renewal of state commodity reserves, which were abolished in 2003. In February 2022, the Government of Montenegro adopted information on the need to form state commodity reserves, which proposed three models: 1) commodity reserves abroad, which are managed from Montenegro; 2) commodity reserves in Montenegro, which implies the construction of infrastructure and the formation of management bodies 3) combined model. First of all, the State Commodity Reserves should provide energy, basic foodstuffs and raw materials to respond to various disturbances. In addition to the intervention role, they can be an incentive and support for the increase of domestic food production, considering that the import of food, for example, in 2019, was 474 million euros, which is even 60 million euros higher than the total export of all goods from Montenegro. In this way, dependence on imports would be buffered, the economy would be strengthened, and the functioning of critical subjects would be ensured, which would strengthen the resilience of the entire society. In order for the State Commodity Reserves to serve the purpose of strengthening society's resilience, it must not be just an arbitrary political decision, but a comprehensive assessment of needs and opportunities conducted in accordance with a clearly defined methodology.

A possible model of the development process of the CER system in Montenegro

Starting from the obvious weaknesses and the need to improve the existing CIP concept, the question arises whether Montenegro and other countries of the Western Balkans should have waited for the completion of the entire process of CER regulation by the EU and the adoption of the CER Directive, or whether they should have already begun to consider the introduction of this concept and catch up first of all with the needs of national security.

From the point of view of the authors of this paper, starting from their own lessons learned from previous crises and the actions of relevant international organizations for this area, Montenegro should have already started a national evaluation of the CIP concept. The evaluation should have started no later than when the EU prepared the proposal for the CER Directive and until the adoption of the CER Directive, the National Concept of CER should have been prepared, so as not to be late for the numerous challenges, risks and threats, which in the modern global world are becoming more and more diverse, changing faster and mostly affecting ordinary people. In support of this, it should be pointed out that the CER Directive, respecting national specifics, gives the possibility of a more flexible creation of the national concept of CER. Also, the thresholds for determining critical entities for the needs of the Union are quite high, so in the countries of the region, and especially in Montenegro, many social and economic entities of national vital importance would remain outside the CER concept. Therefore, the national thresholds for the resistance of critical entities should be lower, that is, the list of critical entities for national interests should be expanded.

Montenegro has already declaratively accepted the concept of strengthening resilience in the DRR Strategy (Strategija; 2017). Also, in the Voluntary Mid-Term Report of Montenegro on the implementation of the Sendai Framework, resilience is highlighted as one of the recommendations for the realization of the outcomes and goals of the Sendai Framework, and one of the main priorities for strengthening the CER of Montenegro is its membership in the EU (Božović et al., 2022).

So, it is no longer questionable whether CER should be developed, but it is rather, how and to what extent? From the previous presentation, we have seen that all existing systems from physical and technical protection, CIP to CER were evaluated in accordance with the requirements of the time, and their establishment was a planning process. That process in theory and practice, as we could see, involves several steps, i.e. phases, from analysis, through conceptualization, normative-legal regulation to the development of plans and their implementation in practice. Errors in steps or skipping certain steps often produce numerous anomalies or create the impossibility of implementing it in practice. Experience shows us that analysis and conceptualization are most often skipped and it goes directly to legal regulation, by rewriting the legal solutions of other countries without taking national specifics into account. Therefore, our intention is, starting from the achieved level of development of the Security System, to try to point out a possible model for the development of the CER system in Montenegro.

By analyzing the Directive - defined technical and organizational measures to strengthen the resilience of critical entities, it can be concluded that a part of the measures in Montenegro have already been implemented through the application of other laws and strategies (the Law on Confirmation of the Paris Agreement; the Law on Physical and Technical Protection of Persons and Property which is not provided by the state: DRR Strategy; Law on protection and rescue, Law on CIP, National strategy proposal in the field of climate change, etc.). Of course, the existing conceptual and normative-legal framework needs to be amended and supplemented in accordance with the new requirements. The analysis shows that the biggest problem for establishing the concept of resilience is the lack of a concept of business continuity of critical subjects, which, according to the author, represents the basic value of the CER concept.

It should be mentioned that Montenegro, like other countries in the region, has some experience of applying a type of business continuity concept of critical subjects, in the form of the functioning of the economy and social activities during the war (from the period of the SFRY), and today, on a reduced scale, the holders of defense preparations are planning actions to secure facilities, products and services of special importance for the defense (Zakon o odbrani). However, it can be said that the concept of business continuity, which would serve to strengthen the integrity of critical entities in Montenegro, does not exist today. Given that BCMS and CER are new mechanisms in the security system in Montenegro, it is necessary to integrate them into the existing system, that is, to harmonize the entire system and adapt it to new circumstances. Practice indicates that the introduction of new mechanisms should be the product of the analysis of the existing situation, conceptualization and normative legal arrangement of the new system as shown in the picture below for the current circumstances in Montenegro.

Therefore, the process is best started with the Strategic Review of the Security System of Montenegro (Božović: 2008: 101-108 and Božović: 2009: 73-80), which would have as its goal the development of the Crisis Management System Concept. Considering that in December 2021, Montenegro prepared the Disaster Risk Assessment, and the Disaster Risk Management Capacity Assessment, which included the analysis of the risks and capabilities of economic and non-economic facilities and institutions (critical entities) is in its final phase, they should be used as a starting point for designing CER. This is supported by the fact that the aforementioned estimates were made in accordance with the Guidelines for reporting on disaster risk management (Article 6 paragraph 1 point d, Decision No. 1313/2013/EU (2019/C 428/07), which Article 5 also prescribes in the CER Directive.

Conceptualization of business continuity management as novelties and unknowns should be started immediately in order to create the basis for its inclusion in the concept of CER and in general the concept of crisis management in the working phase. At the beginning of the development of the business continuity concept, the development of the CER concept also begins, and that process must be interactive. Also, this process must be interactive with the updating of the DRR Strategy of Montenegro, which, in accordance with the Sendai Framework, will begin soon. Considering the mentioned novelties and the expansion of the security system and the concept of crisis management in Montenegro with new elements, it would be necessary to reorganize the system, and we consider the formation of civil protection as the optimal solution. In principle, civil protection would include, in addition to the already existing protection and rescue system, the new CER system, and as a joint function, the early warning and decision-making system and other elements aimed at reducing the risk of disasters. As seen in the image below, the entire design process requires interaction and coordination throughout the design process.

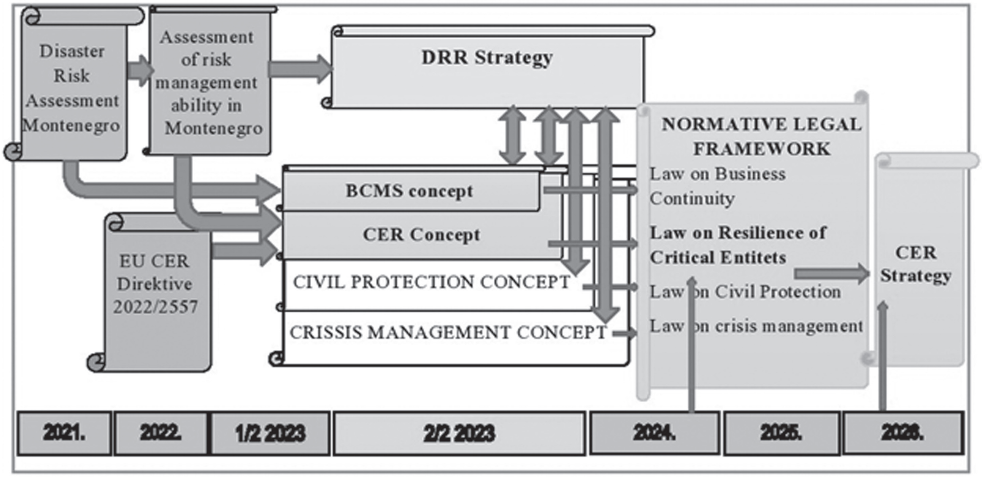

Disaster Risk Assessment Montenegro
Assessment of risk management ability in Montenegro
DRR Strategy
BCMS concept
CER Concept
CIVIL PROTECTION CONCEPT
CRISSIS MANAGEMENT CONCEPT
EU CER Direktive 2022/2557
NORMATIVE LEGAL FRAMEWORK
Law on Business Continuity
Law on Resilience of Critical Entitets
Law on Civil Protection
Law on crisis management
CER Strategy
2021.
2022.
1/2 2023
2/2 2023
2024.
2025.
2026.

Figure 2. A possible model of the development process of the CER system in Montenegro

Only after the phase of conceiving and creating a complete picture of the functioning of the crisis management system and its subsystems, it is necessary to move to the phase of normative - legal regulation and reorganization of the complete crisis management system and its subsystems through amendments to existing laws and drafting new ones (Law on CER, Law on Crisis Management, Law on Civil Protection, Law on Fire Protection - firefighting and others). Also, an important document that should be adopted for the effective establishment of the system is the Program for the Development of the Crisis Management System and all its subsystems in order to define the steps, a realistic time frame, and provide the necessary funds for its establishment. Considering that it is a complex system in which numerous subsystems function, whose activities and plans overlap to a large extent, this can lead to confusion and additional burden on subjects, therefore, it is necessary to prepare CER planning methodologies with unique planning forms.

Conclusion

Montenegro recognized the importance of CIP and treated it in strategic documents, passed the Law on CIP in 2019, as well as the Regulation defining the criteria for determining CIP, designated the competent authority, started implementing the CIP by conducting training and appointing responsible persons at operators, but until today, this concept has not fully taken root. Meanwhile, due to the COVID-19 pandemic and the war in Ukraine, numerous countries and relevant international organizations were forced to replace the existing CIP concept with the CER concept, as the EU did with the adoption of (CER) Directive 2022/2557 in December

2022. This directive imposes obligations on Montenegro, as a candidate for EU membership, to harmonize legislation by October 2025, and to adopt a strategy for strengthening the resilience of critical entities by January 2026. It is obvious that the given deadlines for the implementation of the CER Directive are quite flexible.

However, the carried out analyses indicate that precisely due to this, the countries of the Western Balkans are late in reducing the risks of threats that affect them, because the modernization of the system is not approached in accordance with their national needs, but most often as an obligation to relevant international organizations. Also, research shows that new EU directives are most often implemented in practice without prior implementation of impact analysis and conception, and at the last moment they are directly regulated by laws. Examples from practice have shown that due to such abbreviated procedures in the implementation of directives regulating systemic issues, major problems arise later.

Taking into account the importance of the CER concept for reducing the risk of disruption in modern society, it is necessary for Montenegro to start preparing the national CER concept in a timely, planned and organized manner because it is a very complex process, which will require numerous activities and a lot of time for its full implementation.

Given that CER is a complex multidisciplinary concept, which includes several measures, some of which are, for example, physical and technical protection of buildings, protection and rescue from natural as well as technical and technological disasters already implemented through other laws, the biggest challenge is the establishment of a business continuity management system, because it is a new concept, which is why the focus of engagement should be aimed in that direction. In addition, the analyses indicate that in the circumstances of the introduction of new elements into the system, a reorganization of the entire existing security system is needed. The steps already taken to establish the commodity reserves as one of the instruments of business continuity and supply speak of the urgency of the action.

Starting from the requirements set by the CER Directive and the already achieved level of development of elements to strengthen CER, we proposed a model of the implementation process based on the development of concepts before normative editing. The model, in addition to concrete steps for developing the CER system and BCMS, included the reorganization of the security system, introducing as a possibility the development of the civil protection and crisis management system, which should undergo changes. In particular, it should be emphasized that the model is integrated into a realistic time frame and implies interaction with other processes within the framework of disaster risk reduction.

REFERENCES:

Božović, D., Tmušić, Lj., and Palajsa, T, Montenegro's Voluntary National Report for the Midterm Review of the Implementation of the Sendai Framework for Disaster Risk Reduction 2015-2030 (MTR SF), Podorica, September 2022.
https://sendaiframework-mtr.undrr.org/publication/montenegro-voluntary-national-report-mtr-sf

Božović, D. (2008) Studijski pristup reformi sistema bezbjednosti, časopis Perjanik, Policijska akademija Danilovgrad, broj 17/18, str. 101. – 108;

Božović D. (2009) Sistem kriznog upravljanja, časopis Perjanik, Policijska akademija Danilovgrad, broj 19/20, str. 73. – 80;

Critical Infrastructure Emergency Risk, Management and Assurance, Emergency Management Australia, A Division of The Attorney Generals Department, 2003, str 12.

Direktiva Vijeća 2008/114/EZ od 8. prosinca 2008. o utvrđivanju i označivanju evropske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite, član 2a;

Direktiva (EU) 2022/2557 Evropskog Parlamenta i vijeća od 14. decembra 2022. o otpornosti kritičnih subjekata i o stavljanju van snage Direktive Vijeća 2008/114/EZ;

Holling, C.S., (1973) Resilience and stability of ecological systems. Annual review of ecology and systematics, 4(1).1-23 pp.;

ISDR, U., UNISDR terminology on disaster risk reduction. Geneva, Switzerland, May, 2009.

Introduction to Business Continuity [online]. Thebci.org. Available at: https://www.thebci.org/knowledge/introduction-to-business-continuity.html;

ISO 22 301:2012, Business Continuity Management

Murray, T.G., (2012) Critical Infrastructure protection: The vulnerability conundrum, Telematics and Informatics, 31;

National Security Strategy and Strategic Defense and Security Review 2015 A Secure and Prosperous United Kingdom, Presented to Parliament by the Prime Minister by Command of Her Majesty, p. 44. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf

OECD-JRC Workshop on “System-thinking for critical infrastructure resilience and security” Paris, 24-25 September 2018 ISSUES NOTE;

Pavićević, O., (2003) Koncept otpornosti u sociologiji. Sociologija, 58(3), 2016. I Klein, R.J., R.J. Nicholls, and F. Thomalla, Resilience to natural hazards: How useful is this concept? Global Environmental Change Part B: Environmental Hazards., 5(1), pp 35-45;

Recommendation of the council on the governance of critical risks adopted on 6 may 2014, www.oecd.org;

Recommendation of the Council on the Governance of Critical Risks, OECD WEEK 2014, Paris, www.oecd.org;

Sendai Framework (https://www.preventionweb.net/publication/reading-sendai-framework-disaster-risk-reduction-2015-2030);

Smjernice Komisije za izvještavanje o upravljanju rizicima od katastrofa, član 6 stav 1 tačka d Odluke br. 1313/2013 / EU
https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:52019XC1220(01)&from=EN

Strategija za smanjenje rizika od katastrofa sa dinamičkim planom aktivnosti za sprovođenje strategije za period 2018 - 2023. Vlada Crne Gore; Podgorica, 2017;
https://www.gov.me/dokumenta/a9cf7fb1-1c45-4baf-a5bc-5de9a3329be7

The National Emergency Supply Agency (NESA), https://secure.nesa.fi/

Zakon o odbrani (“Sl. list Republike Crne Gore”, br. 47/07, Sl. list Crne Gore”, br. 86/09, 88/09, 25/10, 40/11, 14/12 i 2/17).

Zakon o određivanju i zaštiti kritične infrastrukture, ‘’Sl. list Crne Gore” broj: 72/2019;

Original scientific paper
UDK 004.7:004.8:[341.231.14
UDK 355.45:341.231.14

THE HUMAN RIGHTS-BASED APPROACH TO THE GOVERNANCE OF EMERGING TECHNOLOGIES

Metodi HADJI-JANEV[1]

Abstract: *Emerging technologies have a major impact on the economic, social and environmental welfare across the globe. They are touching every aspect of contemporary human activities with great velocity and volume. While many aspects of these technologies bring positive impacts to our lives, their disruptive nature raises serious governing concerns. One particular aspect that gathered wider attention and has not been addressed properly is the human rights-based approach to governance of the emerging technologies. This article, therefore, represents an effort to bring greater attention to the important aspect (human rights protection) that should not remain overlooked in future debates on the subject.*

Key words: *Human rights-based approach, Governance, Emerging technologies, Artificial Intelligence, Privacy, National security.*

Introduction

Emerging technologies include a variety of technologies such as educational technology-Machine learning, information technology, nanotechnology, biotechnology, robotics, and artificial intelligence-AI. While these technologies bring many positive socio-economic and security aspects there are many disturbing aspects that are frightening and even challenge human existence. Governing these technologies, therefore, is of paramount importance, to mitigate their negative effects and exploit the positive ones.

This article is an excerpt of the ongoing research on the impact of emerging technologies on human rights and their applicability in the context of governing these technologies. The article starts by drawing the conceptual framework of the debate by providing a narrative framework of what constitutes emerging technologies. It also provides a working framework for the governance of these technologies and the meaning of the human rights-based approach.

After setting the conceptual framework for discussion, the article provides a brief overview of the contemporary efforts to address the governing aspects of emerging technologies, by emphasizing the overlooked issue of human rights. It continues with an attempt to debunk the reasons to diverge from a human rights-based approach to the governance of emerging technologies. In this section, the article tackles some of the reasons that obstruct the human rights-based approach to be central in governing emerging technologies. Here the article argues that the quest for human rights promotion without the proper capacities by the promotors may feed the opposition to a human rights-based approach in their attempts to govern emerging

[1] Associate Professor, Miltary Academy "General Mihailo Apostolski-Skopje, Associated member of the "Goce Delchev" University Shtip

technologies. This is followed by some of the improperly perceived and argued practical reasons for omitting human rights in governing the efforts of emerging technologies. Finally, it brings on the hottest topic in the applicability of human rights to the governance of emerging technologies which is the clash of the concept of universalism and cultural relativism.

After providing some rationale that debunks the reasons for hindering the human rights-based approach in governing emerging technologies, the article offers a way forward, for applying the human rights-based approach to the governance of emerging technologies.

The rise of emerging technologies, the governance of emerging technologies and the concept of a human rights-based approach

There is no general consensus or a list of what one means when referring to the term emerging technologies. This may be understandable given that these technologies' development, practical applications, or both are still largely unrealized. In fact, the velocity and the volume with which emerging technologies are developing and applied are exponential. The former may be understandable given that these technologies are generally new, but also include older technologies finding new applications.

Emerging technologies are characterized by radical novelty (in the application even if not in origins), relatively fast growth, coherence, and prominent impact. However, uncertainty and ambiguity, also follow these technologies and generate skepticism, opportunism and extreme efforts to ban certain segments in total. For some, emerging technologies are those technical innovations that represent progressive developments within a field for competitive advantage (International Congress Innovation and Technology XX., 1997). Others assert that emerging technologies represent "a radically novel and relatively fast-growing technology characterized by a certain degree of coherence persisting over time and with the potential to exert a considerable impact on the socio-economic domain(s) which is observed in terms of the composition of actors, institutions and patterns of interactions among those, along with the associated knowledge production processes. Its most prominent impact, however, lies in the future and so in the emergence phase is still somewhat uncertain and ambiguous." (Rotolo, December 2015).

Another important element to consider when discussing emerging technologies is the process of convergence of technologies. Converging technologies represent previously distinct fields that are in some way moving towards stronger interconnection and similar goals. New technological fields may result from the technological convergence of different systems evolving towards similar goals. Convergence brings previously separate technologies such as voice (and telephony features), data (and productivity applications) and video together so that they share resources and interact with each other, creating new efficiencies. For example, deep fakes use a form of artificial intelligence called deep learning to make images of fake events. (Sample, January 12, 2020). However, the opinion on the degree of the impact, status and economic viability of several emerging and converging technologies varies.

For the purpose of this debate, we will conclude that Emerging technologies include a variety of technologies such as educational technology-Machine learning, information technology, nanotechnology, biotechnology, robotics, and artificial intelligence-AI.

The dual nature of these technologies, i.e. that they are easily manipulated for commercial and political purposes, along with their positive general social benefits, have turned great attention in recent years. The EU Competence Centre on Foresight-an institution oriented to anticipatory culture in the EU policymaking process has already addressed the dual-use nature of these technologies labeling them as dual-use technologies. (Competence Centre on Foresight, June 7, 2019). In their foresight, the EU Competence Centre concludes that technological advances had so great an impact on security, in a way that not only increases the nature and level of threats but also for the possibility of providing the means to address the threats.

Hence, combining efforts of leaders in academia, industry and government have struggled on various forums and through various mechanisms to find governance solutions for rapidly changing technologies. These discussions have covered the broadest possible range of technologies and scientific study, including nanotechnology, artificial intelligence, robotics, autonomous vehicles, the internet of things, human-machine interfaces, neuroscience, synthetic biology, genomics, personalized medicine, telemedicine, human enhancement, gene editing, surveillance, national security, virtual and augmented reality, blockchain, autonomous weapon systems and so on. (See for example ASU May, 2022).

The governance of these technologies thus refers to the act or process of governing or overseeing the control and direction of something (such as a country or an organization) (see Merriam Webster). Similarly, the University of Oxford-based Programme on the Governance of Emerging Technologies is focused on investigating legal, ethical, and social aspects of AI, machine learning, and other emerging information technologies. (Oxford Internet Institute, 2023).

Democratic governance of emerging technologies is unimaginable without the human rights-based approach. Regardless of the contemporary competition and diverging visions of what democratic governance means, at least narratively, both liberal democracies and current revisionist challengers in the ongoing geostrategic competition (seen as autocratic regimes by the liberal democracies, Russia and China) claim that practice of democratic governance. (see for example Elving February 6, 2022). Although the UN does not advocate for a specific model of government, it promotes democratic governance as a set of values and principles that should be followed for greater participation, equality, security and human development (United Nations, accessed February 2023). Democratic governance is the bedrock of the OSCE system of values and standards. It is a system of government where institutions function according to democratic processes and norms, both internally and in their interaction with other institutions (OSCE, accessed March 5, 2023).

In the democratic governance context, the human rights-based approach refers comprehensively to the full range of indivisible, interdependent and interrelated rights: civil, cultural, economic, political and social. Rights-based approaches also focus on the development of adequate laws, policies, institutions, administrative procedures and practices, as well as on the mechanisms of redress and accountability that can deliver on entitlements, respond to denial and violations, and ensure accountability. They call for the translation of universal standards into locally determined benchmarks for measuring progress and enhancing accountability (Sagasti 2004). To simplify and relate to the contextual debate, the human rights-based approach will represent developing the capacity of duty-bearers to meet their obligations and encourages rights holders to claim their rights. Moreover, we will consider that The Human Rights Based Approach is underpinned by five key human rights principles: Participation, Accountability, Non-discrimination and Equality, Empowerment and Legality.

The end of the Human Rights Era and the Rise of Emerging Technologies?

The evolution of Human rights reflects the long struggle of human beings to achieve what today is entrenched in the international law for human rights. From 539 BC when the troops of Cyrus the Great conquered Babylon, through Magna Charta in 1215, the U.S. Bill of Rights (1791), the French Declaration of the Rights of Man and of the Citizen, adopted in 1789, the first three Geneva Conventions and the Hague Conventions (seeking to protect human rights even in times of war) through the UN, the Universal Declaration of Human Rights and the International Covenants on Economic, Social and Cultural Rights and on Civil and Political Rights (known as the International Bill of Rights), the struggle had evolved into the principles and standards that generate obligations and responsibilities to the states around the globe, the institutions that they have formed including corporates that underpin their wellbeing (Sutto, 2019). As a result, today it is broadly accepted that human rights are inherent to all human beings, regardless of our nationality, residence, sex, sexual orientation and gender identity, national or ethnic origin, color, religion, language or any other status. What is also important to mention from the historical perspective is that the ideological ardent belief that human rights would become drivers to global stability prior to WWII, had largely been materialized after the War with the inception of the United Nations (See Maxwell March 18, 2021). This maybe best exemplified in the fact that the Charter of the United Nations does not begin with “we the Nation states”, but rather with “we the people…” (The Charter of the United Nations, 1949). The development and the progress of International law during the Cold War were arguably advanced by the development of Human Rights. In fact, the only consensus of the two major blocks, including the rest of the World (for example, the Non-Aligned Movement), was about the need to develop human rights. As a result, international human rights law crystallized ethical principles into norms that were particularly advanced after the end of the Cold War and the dominance of the victorious Liberal democracy over the socialist ruling.

The emerging situation of protecting individuals against the brutality of some regimes was well-calibrated through a method of balancing the rights of the individual against competing rights and interests using tests of necessity and proportionality. As a result, human rights began to provide the main framework during the processes of governance both for industries and governments. In the meantime, they evolved into the ecosystem for the provision of remedies for breaches. Nevertheless, the rise of emerging technologies and the struggle to govern these technologies seems to defy these trends and generate a void that distances human rights-based approaches in the visions and debates about governing these technologies.

While some efforts to provide guidance or genuine thinking about governing emerging technologies have considered the ethical use of these technologies, most of the emerging technologies governance principles produced by companies, governments, civil society and international organizations fail to mention human rights at all. For example, in its first-ever State of Ethics and Trust in Technology annual report on defining emerging technologies, Deloitte identifies trustworthy and ethical standards and explains different approaches to operationalizing standards, while encouraging actions that can be taken in the short term (Deloitte, 2022). Similarly, four of the EU reports on emerging technologies (molecular biotechnology and artificial intelligence) talk about ethical principles for emerging technologies (Boldt & Orru 2022). Another example, where even human rights law is observed entirely from the aspect of ethics is the UNESCO Recommendation on the Ethics of Artificial Intelligence lists (The UN Educational, Scientific and Cultural Organization, 2021).

At the same time, a 2020 review of 36 prominent sets of AI principles from around the world, authored by a diverse range of governmental and non-governmental bodies, found that only 23 referred to international human rights. Only one-half of the government documents reviewed include any reference to human rights. Five of the 36 sets of AI principles used international human rights as a framework for their work (Fjeld, J. et al. 2020). Similarly, a separate evaluation of 22 sets of guidelines makes no reference to human rights (Hagendorff, 2020).

These and other similar observations unequivocally elevate the question of why the human rights-based approach is not considered during the efforts for governing emerging technologies.

Debunking the reasons to diverge from a human rights-based approach to governance of the emerging technologies

The dominance of the liberal world and the quest of promoting liberal democracy after the fall of communism seems to have caught liberal promotors unprepared. The rightful need to promote human rights as one of the core liberal democratic values demanded promotion from various aspects from policy to philosophical and ethical aspects of human rights, including the promotion of the legalistic aspects of the human rights system. Parallel to these demands, the Track II diplomacy efforts as tools or means were utilized to fuse human rights promotion in most of the post-communist societies along with their liberal democratic values. Given that the Western liberal democracies came victorious after the end of the Cold War through various projects and perpetrators under the Track-II diplomacy framework helped deliberately to spread liberal democratic values across ex-communist states in Eastern Europe. These initial efforts were soon adjusted through an institutionalized approach translated to NATO and EU integration frameworks. As such, with the narrative and image of well-being, the EU and NATO have almost immediately become the desired destinations for many Eastern and Central European nations seeking stability, peace, modernity and prosperity. Hence, the fusion of the collective security idea - desire to feel secure and seek belonging (see for example: (Bourgeois, 2002), the idea of individual liberal democratic freedoms (as opposite of some limitations and determinism entrenched under collectivism to preserve communist ideology) and the liberal democratic values (particularly emphasizing the quest of separation of power to effectively govern, separation of state and political party, political equality and equality before the law) turned into the technology of power translated in the integration processes (given as prerequisites for integration in the later processes). This is when democratization, in fact, was not just an ideological effort, but also a political tool (Madhav, September 27, 2022). Of course, liberal philosophy and moral values were an important part of promoting human rights, as the facilitator in promoting liberal democracy. But when it comes to emerging concepts or dynamics such as governance of emerging technologies, complementary disciplines such as for example, ethics and law (we will refer to this below), or what is just and what is legal, may diverge and generate confusion.

Along the way of these processes, several reasons why governments and the corporate world avoid human rights-based approaches to the governance of emerging technologies have surfaced. Some are the result of political agenda and unintentional side effects to pursue this agenda. Some of these reasons stem from the different interests that corporates and the government share. Other reasons, nevertheless, stem from the different perceptions that are more or less the result of tradition, values and expectations (i.e. cultural). Although others have similar views and approach in this regard, we have summarised these reasons as follows:

- The quest for human rights promotion without the proper capacities by the promotors;
- Advocacy for human rights inhibits innovation spirit and
- The ongoing clash between the universalist vs cultural relativist concepts of human rights.

The quest for human rights promotion without the proper capacities by the promotors. The demand to expand liberal democratic values grew exponentially as communism failed. It could be argued that this to a certain degree caught the liberal world quite unprepared. While rightfully soft diplomacy measures, tools and techniques were utilized to demonstrate and disseminate liberal democratic values, not every one of these disseminators seemed to be prepared for the purpose. Hence, in the efforts to provide the required service and help the process of democratization, the promotion of human rights rightfully required ethical and philosophical, including policy creation experts. Nevertheless, it could be argued that the lack of legal expertise, intentionally or not, influenced the supporters to become leaders. Hence, all of the sudden, the human rights disseminators were all but lawyers and the argument was all but legal. Again it is not that here we argue that other aspects of human rights are not important but that these aspects should not take the lead, particularly not because at the end of the day we are not talking about human ethics, but human rights as legally established principles and standards at international level.

One way to support the thesis of this unintentional divergence may be to look into the portfolios of various professions and the requirements of the jobs (leading positions) of various projects well intended to help human rights promotion. Experts in policy, ethics, humanism, development etc. substitute lawyers in many aspects of promoting human rights in general. Similarly, this trend has been reflected to a certain degree in governing of emerging technologies, where IT experts lead policy creation without proper experience (of course with respected exclusions).

One of the results of these dynamics is mixing apples and oranges. Today, many corporates, organizations and institutions (as we have already underlined above) believe that ethics holds all the answers to human rights. With this approach, they introduce conceptual confusion, where human rights are regarded as an element of ethics rather than parallel to it. This in the long run stimulates competition instead of the complementary relationship between the two concepts. Conflicts between norms at the end harm legal certainty and predictability, an important part of governance, something on which states, businesses and individuals rely.

In practice, the acquiescence of ethics (as compensation for the lack of proper human resources) inhibits civil society actors' ability to hold other actors (wrongdoers) accountable. As the Carnegie Council of ethics put it "some technology companies face undertaking 'ethics-washing' for reputational purposes (Carnegie Council for Ethics in International Affairs, accessed March 2 2023). Others have used different techniques to undue influence on some ethics researchers through funding (Williams, 2019). On the other hand, the challenge is that Courts and tribunals, one of the powers in the democratic world that ensure democracy in practice, do not allocate remedies for compliance with ethics. In this line, while ethical principles are intended to ensure that technology reflects moral values, as Wagner argued "a focus on ethics may minimize the appetite for legal regulation" (Wagner, 2018).

Thus, to summarise, it would be naïve to believe that reaching a universal agreement on emerging technologies ethics without reference to the already-agreed human rights framework would be easier, or less politically charged. In fact, establishing international agreement(s) on the content of the Universal Declaration of Human Rights – and later the International Covenant on Civil and Political Rights and International Covenant on Economic, Social and Cultural Rights – required worldwide canvassing, expert input, negotiation and political compromise (Lauren, 2011).

Advocacy for human rights inhibits innovation spirit. According to some views, human rights are a speed bump for innovation. The core and framework of Human rights, according to these views prevent an epitomized Silicon Valley business culture, or the well-known - 'move fast and break things' ethos. Accordingly, human rights entail compliance with minimum standards and therefore obstruct innovation by forbidding certain egregious activities, necessary to push things beyond. The truth is that human rights provide an appropriate framework for standards and processes at the international level. The public will continue to grow weary of perceived abuses by tech companies and will favor businesses that address economic, social, and environmental problems. In general everyone that is involved in innovation wants to know how he/she can meet shared standards and inspire trust in their products. The businesses are the same in this context. Development and use of emerging technologies in a regulated and trusted manner foster customer trust and minimize potential costs and time expended in litigation at a later stage.

In the societal evolution context, the quest for systematic change favors smart entrepreneur leadership for sustainability and practicality. As Hemant Taneja analyzed in an imagined interview for Harvard Business reviews "Suppose we spoke to an entrepreneur working on human longevity. We would need to see a vision—and a minimum virtuous product—that addressed disruption in labor markets through automation (what does the world look like when people live longer and have less access to work?) and disparity in access (will society allow a world in which the wealthy live 2X as long as the middle class? 3X as long as the poor? Should it?). The best leaders of tomorrow will see these links and plan for them from day one". (Hemant, January 22, 2019).

The contradiction of concepts of Universalism and Cultural Relativism. The contradiction of concepts of Universalism and Cultural Relativism has become a prominent source of the discourse that challenges the human rights-based approach to the governance of emerging technologies. This rift, nevertheless, is so essential that it elevates to the level of challenging the approach to the whole liberal democratic framework and with that understanding of human rights. The struggle to pursue the proliferation of liberal democratic values (regardless of the intentions, predominantly positive of course) ended up blurring the lines between the Western efforts to help the process and the danger of universalizing these efforts as general moral values (see for example: Corella, December 2018). The latter has become particularly important with the rise of authoritarian "revisionism" whose core argument is entrenched in the idea to revise the so-called rule-based order, as these leaders see, dominated by the liberal democratic idea (Stent, February 2020). Similar echoes (although not opportunistic as the authoritarian revisionists) have dominated human rights legal and political discourse for quite a while.

The dilemma of international protection of human rights is shaped by the the ideological conflict between Universalism and Cultural Relativism. Simply put, the concept of Universalism holds that each human being possesses certain inalienable rights simply because he or she is a human, regardless of the national background, religious or political views, gender, or age. The proponents of this concept claim that "international human rights like rights to equal protection, physical security, free speech, freedom of religion and free association are and must be the same everywhere (Lawteacher.net, March 2023).

The cultural relativism protagonists argue that Cultural relativism is based on the stable conception of culture, which fails to recognize the flexibility of culture for social changes and ideological innovations. The best example to explain the contextual discourse is the Chineses Social Credit System. According to

Chinese officials, the system is understood as a tool for improving internal security and market economy. However, it is not clear to what extent the system protects human rights and the rule of law (Gavazzi, 2020).

For the West, the list of Chinese human rights abuse with this mass surveillance tool (an emerging technology application) is indefinite. Those violations include torture and other abuses in the criminal justice system, the lack of media and internet freedom; land rights, labor rights, 'birth planning' policies; and various kinds of discrimination, including against the physically or mentally disabled, the persecution of dissidents, communities of faith and minorities (Pils, 2018). Nevertheless, the Chinese understanding of human rights differs from the Western one. Notably, the PRC emphasizes collective rights more than individual freedoms by saying that too many freedoms lead to chaos. Pursuing this position, the geopolitical influence that China is aiming for in order to reshape the international understanding of human rights and the rule of law, is on top of economic interests. Regarding the rule of law as the essence in approaching human rights, the problem goes to the core and that is the definition of "what the rule of law is". Despite the fact that the term has been clarified by UN officials and by several International organizations, it seems that there is no universal consensus. However, while the Chinese Constitution states its own supremacy, it is clear that the Chinese Communist Party-CHP codes are much more important. Consequently, equality before the law and the principle of division of power are not effective in China which is maybe the core error in the Chinese democratic argument or a source for CHP's mascarade. (Liang et al., 2018, p. 415-453)

Without getting into deeper debate on the Chinese geostrategic competition ambitions and the abuse of the power vacuum to challenge international architecture, the idea that the clash of the "universalistic" views with "cultural relativistic" views in human rights is one of the reasons that obstruct the human rights-based approach to the governance of the emerging technologies.

Way forward, Appying the human rights-based approach to the governance of emerging technologies

For now, there are no international human rights treaties designed to address the impact of emerging technologies (Council of Europe (2022). This nevertheless, does not mean that the existing human rights laws do not apply to emerging technologies. For example, in tackling the issue of AI, the former UN High Commissioner for human rights, Michelle Bachelet, clarified that "AI can have significant impacts on the implementation of many human rights, including privacy, health, education, freedom of movement, freedom of assembly and association, and freedom of expression" (United Nations High Commissioner for Human Rights, 2021). She went further to note "that inferences and predictions about individuals made by AI may profoundly affect not only those individuals' privacy but also their autonomy, and may raise issues regarding freedom of thought and opinion, freedom of expression, the right to a fair trial and other related rights" (UNHCHR 2021, p.17) Uses of faulty data may result in bias or discrimination (UNHCHR 2021, p.19), as may faulty AI tools. Uses of AI in the criminal justice process may lead to violations of the rights to privacy, fair trial, freedom from arbitrary arrest and detention and even the right to life (UNHCR 2021, p.24). The human rights-based approach is and should be applicable in almost all of the disputed and challenged areas mentioned in UNHCHR's argument. The human right to privacy, for example, requires that any processing of personal data should be "fair, lawful and transparent, based on free consent or another legitimate basis laid down in law". Data may be held, but only for a limited period and for specific purposes. These purposes cannot be changed without an institutionalized process that hardens easy democratic manipulations. Furthermore, the held data must be stored in a proper and secure way, and sensitive personal data should enjoy heightened protection. The right to privacy also stipulates that a person should know that his/her/its personal data has been retained and processed and that that person has the right both to rectify or erase their personal data and limit how it is used. Privacy further entails that individuals must not be exposed to mass surveillance or unlimited profiling. Personal data should not be transferred, particularly overseas, unless similar standards are upheld by the recipient of that data (United Nations High Commissioner for Human Rights, 2018).

Besides international bases, many regional human rights international legal instruments also entail applicability to privacy and thus the Human rights law is already the widely accepted basis for most legislation protecting privacy providing background for a human rights-based approach to privacy. For example, The EU General Data Protection Regulation (GDPR) is founded on the right to protection of personal data in Article 8(1) of the EU Charter of Fundamental Rights, which in fact, is an aspect of the right to privacy in earlier human rights treaties (Jones, January 2023). Privacy and data protection is one of the European Commission's Seven Principles for Trustworthy AI, while most statements of AI principles include a commitment to privacy (Fjeld et al. (2020).

Another reason for a human rights-based approach to governing emerging technologies stems from the international human rights law's principles and standards relevant to equality. Principles and standards enshrined under international human rights law set a framework that all individuals' rights be respected and ensured. Equality and nondiscrimination are particularly articulated in Article 2(1) of the International Covenant on Civil and Political Rights (International Covenant on Civil and Political Rights, 1966, Article 2(1). Regional instruments of International human rights law add further to the non-discrimination background by forbidding discrimination in all circumstances, rather than merely in the implementation of the rights. In Protocol 12 to the European Convention on Human Rights and Articles 20 and 21 of the European Charter of Fundamental Rights discrimination it is forbidden "without distinction of any kind, such as race, color, sex, language, religion, political or another opinion, national or social origin, property, birth or another status (European Convention on Human Rights, 1950). European law on human rights forbids prohibitions against not just direct discrimination (i.e. treating people differently on prohibited grounds), but indirect discrimination (i.e. treating people the same, but in a way that puts people from a protected group at a disadvantage without an objective justification) and structural discrimination (i.e. creating structural conditions in society that prevent all groups from accessing the same opportunities). Just to be sure providing a legal framework and obligations for equality does not always mean treating everyone the same. Instead, European provisions for the discrimination law provide structured tests for assessing and preventing unlawful treatment.

The rapid development of emerging technologies has brought the freedom of thought, inter alia, to the center of legal debate, particularly in the context of the applicability of human rights principles and standards. Individual autonomy is well protected as privacy under the framework of international human rights law. This means that a person has the right to freedom of thought and the right to hold opinions without interference, as well as the better-known and -understood rights to freedom of expression, freedom of assembly and association, and freedom of conscience and religion. Mental integrity as a right is also protected under the EU Charter of Fundamental Rights. Prior to recent technological developments, the rights to freedom of thought and opinion were underexplored. Nevertheless, given the velocity and the volume of the dynamics and development of emerging technologies, these areas generate further debate and as a result, there are new guidelines emerging. For example, the UN Special Rapporteur on freedom of religion or belief has recently issued guidance on freedom of thought (UN Special Rapporteur on Freedom of Religion or Belief, October 2021, paras 68–72).

The increased monetization of children empowered by emerging technologies has lately put emphasis on Children's rights too. The application of the human rights-based approach to the governing of emerging technologies in children's contractual rights goes beyond the questions over privacy and the ability of minors to give consent when providing personal data. The UN Committee on the Rights of the Child has called for practices that rely on "neuromarketing" and "emotional analytics" to be prohibited from direct or indirect engagement with children. Furthermore, it also called nation states "to prohibit manipulation or interference with the child's right to freedom of thought and belief through emotional analytics and interference" (UN Committee on the Rights of the Child, March 2, 2021, para. 42).

Although there is a substantial background to apply a human rights-based approach to governing emerging technologies, the considerations mostly focusing on the impacts of surveillance, privacy, discrimination and autonomy do not provide a sufficient framework to take into account all potential issues of manipulation and human rights abuses. Commercially designed algorithms (easily manipulated for political purposes as well) nested under emerging technologies allow for billboards to adapt advertising according to the reactions of people walking past, stores that adapt their advertising and marketing after capturing shoppers' reactions in real-time or bots that reflect users' emotions in order to influence their decision-making. While the former is not wrong, legally per se, in a system where corruption and organized crime reside and blend illiberal practices, this may turn into a nightmare for human rights. Hence, it is unequivocally clear that initiatives to set limits on simulated empathy, such as the technical standard under development, further legislative and judicial consideration is needed to establish precisely what constraints the human rights law imposes on the potentially manipulative uses of emerging technologies, and precisely what safeguards it imposes to prevent the erosion of autonomy. The demand for further legal debate in applying human rights-based approach to governing emerging technologies also stems from the challenges discussed above, particularly in the cultural relativism context (please see the debate about culture relativism). For example, in its announcement to phase out emotion recognition from its Azure Face API facial recognition services, Microsoft underlined the lack of scientific consensus on the definition of 'emotions', the challenges of generalizations across diverse populations, and privacy concerns, as well as awareness of potential misuse of the technology for stereotyping, discrimination or unfair denial of services. (Bird, June 21, 2022).

Conclusion

Emerging technologies bring both positive and negative aspects and impacts on our everyday lives. Academic and expert communities, industries and government officials at bilateral, regional and international institutional levels undertake serious efforts to govern emerging technologies such as nanotechnology, artificial intelligence, robotics, autonomous vehicles, the internet of things, human-machine interfaces, neuroscience, synthetic biology, genomics, personalized medicine, telemedicine, human enhancement, gene editing, surveillance, national security, virtual and augmented reality, blockchain, autonomous weapon systems and so on. For now, while democratic governance of these technologies dominates the public discourse and narrative, a human rights-based approach is missing. While some efforts to provide guidance or genuine thinking about governing emerging technologies have considered the ethical use of these technologies, most of the emerging technologies' governance principles produced by companies, governments, civil society and international organizations fail to mention human rights at all. Many reasons contribute to this outcome, the main being the quest for human rights promotion without the proper capacities of the promotors; advocacy for human rights inhibits the innovation spirit i.e. "The human rights are a speed bump for innovation" and "the ongoing clash between the universalist vs cultural relativist concept of human rights". Although there is substantial background to apply a human rights-based approach to governing emerging technologies, the demand for further legal debate is palpable and persistent.

REFERENCES:

ASU, (May 2022), "Conference on Governance of Emerging Technologies and Science (featuring the project on Soft Law Governance of A.I.", available at: https://asuevents.asu.edu/content/conference-governance-emerging-technologies-and-science

Bird, S. (June 21, 2022,), "Responsible AI investments and safeguards for facial recognition", Microsoft Azure blog, https://azure.microsoft.com/en-us/blog/responsible-ai-investments-and-safeguards-for-facial-recognition.

Boldt Joachim, & Orru Elissa, (2022), "Towards a unified list of ethical principles for emerging technologies. An analysis of four European reports on molecular biotechnology and artificial intelligence", Sustainable Futures, Volume 4, 2022, available at: https://www.sciencedirect.com/science/article/pii/S266618882200020X

Bourgeois Y David, (2002) "The Politics and Values of Individualists and Collectivists: A Cross-Cultural Comparison", Digitam Commons, The University of Maine, available at: https://digitalcommons.library.umaine.edu/cgi/viewcontent.cgi?article=1063&context=etd#:~:text=Collectivism%20emphasizes%20the%20primacy%20of,dimension%20calls%20attention%20to%20hierarchy.

Carnegie Council for Ethics in International Affairs, (accessed March 2 2023) 'Ethics Washing', https://www.carnegiecouncil.org/explore-engage/key-terms/ethics-washing

Corella S. Ángeles, (December 2018) "The Political, Legal And Moral Scope Of The Universal Declaration Of Human Rights: Pending Issues", The Age of Human Rights Journal, 11, pp. 1-23 ISSN: 2340-9592 DOI: 10.17561/tahrj.n11.1

Competence Centre on Foresight, (June 7, 2019), "Dual Use Technologies", EU Commission, available at: https://knowledge4policy.ec.europa.eu/foresight/topic/changing-security-paradigm/artificial-intelligence-quantum-cryptography_en

Council of Europe (2022), 'Inaugural Meeting of the Committee on Artificial Intelligence

Deloitte, 2022, State of Ethics and Trust in Technology", available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/about-deloitte/us-tte-annual-report.pdf

Elving Ron, (February 6, 2022), " Beijing and Moscow unite in efforts to redefine democracy itself", NPR, available at: https://www.npr.org/2022/02/06/1078432575/beijing-and-moscow-unite-in-efforts-to-redefine-democracy-itself

European Convention on Human Rights, (1950), Council of Europe, Articles 20 and 21 of the European Charter of Fundamental Rights

Fjeld, J. et al. (2020), “Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI”, Berkman Klein Center for Internet & Society, Research Publication No. 2020-1, http://dx.doi.org/10.2139/

Gavazzi Simone, (2020), “Technology And Cultural Relativism” Social Credit System, Human Rights, and the Rule of Law in China, Master theisis, Lund University

Hagendorff, T. (2020), ‘The Ethics of AI Ethics: An Evaluation of Guidelines’, Minds and Machines, 30, pp. 99–120, https://link.springer.com/article/10.1007/s11023-020-09517-8.)

Hemant Taneja (January 22, 2019), “The Era of “Move Fast and Break Things” Is Over”, Harvard Business Review, available at: https://hbr.org/2019/01/the-era-of-move-fast-and-break-things-is-over

International Congress Innovation and Technology XXI: Strategies and Policies Towards the XXI Century, & Soares, O. D. D. (1997). Innovation and technology: Strategies and policies. Dordrecht: Kluwer Academic

International Covenant on Civil and Political Rights, (1966), Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976, Article 2(1) available at: https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/ccpr.pdf

Jones Kate, (January 2023), “AI governance and human rights, Resetting the relationship”, Chatham House, International Law Programme, available at: https://www.chathamhouse.org/2023/01/ai-governance-and-human-rights

Lauren G. Paul (2011), “The Evolution of International Human Rights”, University of Pennsylvania Press, available https://www.jstor.org/stable/j.ctt46nqdn

Lawteacher.net, (March 2023), “Universalism and Cultural Relativism in Human Rights”, available at: https://www.lawteacher.net/free-law-essays/international-law/universalism-and-cultural-relativism-in-human-rights-international-law-essay.php?vref=1

Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018), “Constructing a Data-Driven Society: China’s Social Credit System as a State Surveillance Infrastructure”, Policy & Internet, 10(4), p. 415-453.

Maxwell David (March 18, 2021), “Fyfe’s closing speech for the UK prosecution at Nuremberg”, available at ‘The Human’s In the Telling’, https://thehumansinthetelling.wordpress.com.

Madhav Ram, (September 27, 2022, “New Order with a Blend of Western Liberalism and Eastern Civilizational Nationalism”, Institute Montagine, available at: https://www.institutmontaigne.org/en/analysis/new-order-blend-western-liberalism-and-eastern-civilizational-nationalism)

Merriam Webster, Governance-Noun, accessed: https://www.merriam-webster.com/dictionary/governance

OSCE, (accessed March 5, 2023), “Democratic governance”, available at: https://www.osce.org/odihr/democratic-governance#:~:text=It%20is%20a%20system%20of,their%20interaction%20with%20other%20institutions.

Oxford Internet Institute, (accessed 2023), “Programme on the Governance of Emerging Technologies” available at: https://www.oii.ox.ac.uk/research/projects/governance-of-emerging-technologies/#:~:text=Related%20Topics-,Overview,and%20are%20shaped%20by%2C%20society.

Pils Eva, (2018), “Human rights in China: A social practice in the shadows of authoritarianism”, Cambridge: Polity, Rotolo, Daniele; Hicks, Diana; Martin, Ben R. (December 2015). "What is an emerging technology?" (PDF). Research Policy. 44 (10): 1827–1843

Sample Ian, January 12, 2020), "What are deepfakes – and how can you spot them?", The Guardian, available at: https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them

Sagasti Francisco, (2004), "A human rights approach to democratic governance and development", OHCHR, Chapter 9, available at: https://www.ohchr.org/sites/default/files/Documents/Issues/Development/RTDBook/PartIIChapter9.pdf

Stent Angela, (February 2020), "Russia and China: Axis of revisionists?", Brookings, available at: https://www.brookings.edu/research/russia-and-china-axis-of-revisionists/

Sutto Marco, (2019), "Human Rights evolution, a brief history", The CoESPU MAGAZINE" nr. 3-2019, p.18, available at: https://www.coespu.org/articles/human-rights-evolution-brief-history

The Charter of the United Nations, 1949, Art.1 available at: https://treaties.un.org/doc/publication/ctc/uncharter.pdf

The UN Educational, Scientific and Cultural Organization (2021), Recommendation on the Ethics of Artificial Intelligence, Paris: UNESCO, section III.1, available at https://unesdoc.unesco.org/ark:/48223/pf0000381137

United Nations, (accessed February 2023), "Democracy", available at: https://www.un.org/en/global-issues/democracy#:~:text=The%20UN%20does%20not%20advocate,equality%2C%20security%20and%20human%20development

United Nations High Commissioner for Human Rights (2021), The Right to Privacy in the Digital Age, A/HRC/48/31, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/21/PDF/G2124921.pdf

United Nations High Commissioner for Human Rights (2018), "The Right to Privacy in the Digital Age", A/HRC/39/29, https://www.ohchr.org/en/documents/reports/ahrc3929-right-privacy-digital-age-report-united-nations-high-commissioner-huma

UN Special Rapporteur on Freedom of Religion or Belief (October 2021), Freedom of Thought, A/76/380, https://undocs.org/Home/Mobile?FinalSymbol=A%2F76%2F380&Language=E&DeviceType=Desktop&LangRequested=False

UN Committee on the Rights of the Child (March 2, 2021,), General Comment No. 25 on children's rights in relation to the digital environment, CRC/C/GC/25,

Wagner Ben, (2018), "Ethics as an escape from regulation. From "ethics-washing" to ethics-shopping?" in Bayamlioglu, E. et al. (eds) (2018), Being Profiled:Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, pp. 84–8, Amsterdam: Amsterdam University Press, https://doi.org/10.1515/9789048550180-016

Williams Oscar, (2019), "How Big Tech funds the debate on AI ethics", New Statesman, 6 June 2019) available at: https://www.newstatesman.com/science-tech/2019/06/how-big-tech-funds-debate-ai-ethics

Original scientific article
UDK 004.738.5.056.5:334.012.64(497.7)

CYBERSECURITY POSTURE RESEARCH IN SMALL ORGANIZATIONS

Neven TRAJCHEVSKI[1]
Goce STEVANOSKI[2]

Abstract: *This study presents the results of empirical research of cybersecurity posture of small organizations in North Macedonia. The results are present as quantitative determined value within a defined taxonomy based on the theoretical foundation of prospect theory and status quo bias. The analyzed quantity is a relation between two key parameters of the cybersecurity posture of an organization, the cybersecurity readiness and the decision makers' perceived risk of cyber-attack. The study also consists of a comparative analysis between these results and the gained results during other studies in EU and USA.*

Key words: *North Macedonia, Cybersecurity, Posture, Risk, NIST.*

Introduction

Cybersecurity is becoming challenging and even existentially important for small enterprises and organizations as never before, as they are shifting towards higher dependence on information technology. The information technology is also the main propulsion which provides their development. Therefore it is challenging to be dependent on information technology which can be vulnerable and can become costly if it is not properly protected. According to (DCMS, 2020) in the UK almost half of the businesses (46%) reported having cybersecurity breaches or attacks within a 12-month period. The small enterprises are considered the backbone of EU's economy and they also account for more than half of Europe's GDP. Taking this in consideration it is very important to estimate their cybersecurity posture and further to implement measures for improvement.

There is no general accepted definition of what is a “small organization”. For example according to the EU definition (EC, 2021) entities are considered as SMEs (small and medium-sized enterprises) if the staff headcount is less than 50 and the enterprise turnover is less than €10m. However this research is not limited to business enterprises but includes also public/ government administration, non-government organizations, utility providers, etc. Therefore the term "small organization" in this study is regarding any organization which is provider of services, regardless of the sector, and it has IT infrastructure consisting of minimum a web site and a local network with less than 50 user stations in the sector that is the focus of the research or in the entire organization.

This study aims to estimate the cybersecurity posture of small organizations in North Macedonia and to make a comparative analysis with the results gained in the EU and USA.

[1] University “Goce Delchev” – Shtip, Military Academy “General Mihailo Apostolski” – Skopje, associate member

[2] University “Goce Delchev” – Shtip, Military Academy “General Mihailo Apostolski” – Skopje, associate member

The need of such study is recommended in the conclusions of the very comprehensive study given by (Eilts, 2020). Therefore, we adopted that a reliable comparative analysis can be done with the results given in (ENISA, 2021) and (Eilts, 2020). In order to make a quantitative and qualitative assessment appropriate for comparison with these studies, this research utilizes the instrument which have been developed within one of them (Eilts, 2020).

Methodology

This study consist of 7 phases/steps in order to give an answer to two research questions: what is the cybersecurity posture of small organizations in North Macedonia and if there is a significant difference in comparison with the EU and the USA. The overview of this research process is presented in Figure 1. In phase 1 we have defined the opened researched questions based on relevant references and we decided that our approach should be in line with the contemporary findings in this field in the EU and the USA. Thus, we agreed that we will use already developed taxonomy for evaluating the cybersecurity posture and the already developed instrument within the (Eilts, 2020) in order to be able to make relevant comparisons with the EU and the USA, phase 2 and phase 3. Furthermore, in phase 3 we have executed a quantitative study, following by data analysis of the gained data from 20 small organizations in North Macedonia. At the end, we have made a quantitative and qualitative comparison with the other studies in the EU and the USA in phase 6 and the last phase was to derive certain conclusions about the further strategic direction of managing the cybersecurity posture in North Macedonia, as well as certain direction for further research. Enclosed is the description of the most important elements of the implemented taxonomy and research instrument.

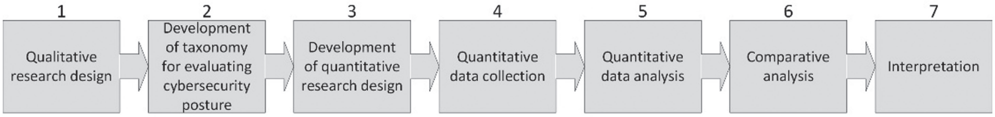

1
Qualitative research design
2
Development of taxonomy for evaluating cybersecurity posture
3
Development of quantitative research design
4
Quantitative data collection
5
Quantitative data analysis
6
Comparative analysis
7
Interpretation

Figure 1. Research study phases

This research utilizes the developed new construct and research instrument, a taxonomy for assessment of cybersecurity posture **Cybersecurity Preparedness-Risk Taxonomy (CyPRisT)**. The new construct is a relation of **two key parameters** of the cybersecurity posture of an organization, the **cybersecurity readiness** and the **decision makers' perceived risk of cyber-attack**.

Cybersecurity Preparedness-Risk Taxonomy (CyPRisT)

The base of the newly defined CyPRisT is in social theories of risk management. This is supported by published findings in papers like (Gupta & Hammond, 2005), which presents that businesses were affected by the decision makers' indifference towards cybersecurity threats while they were focused on doing the primary business activities. Such theories are the *Prospect theory* and *Status quo bias*. The Prospect theory of Kahneman & Tversky offered new insight into why nonoptimal decisions are made when they are framed in different ways. (Bazerman, 1984) analyses the framing effect of the Prospect theory and he gives his findings that decision makers' tend to be risk averse in positively framed situations, while being risk seeking in negatively framed situations. In addition (Tversky & Kahneman, 1991) presented that the retention of the status quo is an option in many decision problems referring to the status quo bias effect and that there is relation between the status quo bias and the loss aversion. According to (Tversky & Kahneman, 1991) the value function given on Figure 2 illustrates the prospect theory in the decision-making process where the reference point is intersect between the subjective value of the perceived gain or loss. Furthermore, (Tversky & Kahneman, 1992) introduce their new Cumulative prospect theory, which applies to uncertain as well as to risky prospects with any number of outcomes, and it allows different weighting functions for gains and for losses.

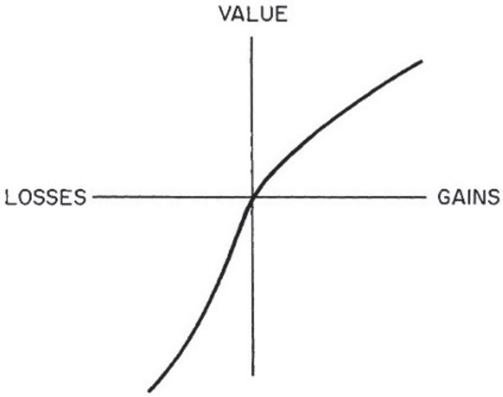


Figure 2. An illustration of a Value Function (Tversky & Kahneman, 1991)

The review of Prospect theory and Status quo bias literature provides the theoretical foundations for the relationship between *risk management activities* and *decision makers' perceptions* of threat. Applying these theoretical lens in the field of information systems security defines the taxonomy quadrants of the CyPRisT. Measuring the cybersecurity preparedness, as well as the decision makers' perceived risk of cyber-attack and further classifying them in the CyPRisT gives a representation of the cybersecurity posture. There are four quadrants in the CyPRisT as shown in Figure 3. The first quadrant *indifference* (Q1) is explained by the decision maker's unwillingness to abandon the status quo and they are at risk of loss due to a cyber-attack. The second quadrant *susceptible* (Q2), refers to risk-seeking behaviors where the decision maker's awareness of cyber threats and possible loss exists, but there is not actions toward mitigation of cyber threats.

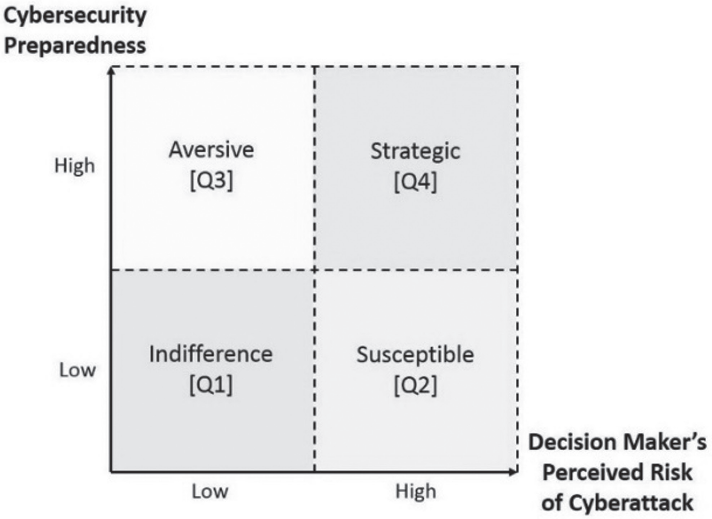


Figure 3. Cybersecurity Preparedness-Risk Taxonomy - CyPRisT (Eilts, 2020)

The third quadrant *aversive* (Q3), refers to the loss aversion effect based on the choice to become risk-averse based on the perceived point of reference for cyber risk and potential loss. In this case the decision maker is less focused on managing of the cyber risk due to low perceived risk. The fourth quadrant *strategic* (Q4) is a posture where there is balanced ratio between the understanding cyber risk and the actions for mitigating the threats.

Cybersecurity Preparedness

The cybersecurity preparedness refers to risk management that includes both cybersecurity readiness and resilience. Assessment of this quantity is based on the application of NIST Cybersecurity Framework activities (NIST 2018). Within the framework these activities are grouped in five functions: Identify, Protect, Detect, Respond and Recover. The activities are transformed in questions in an iterative process of the Delphi method engaging certain number of subject matter experts and also validated and weighted (Eilts, 2020). This process resulted in 70 (Yes=1/No=0) questions within the five NIST functions. During this process each question is also accompanied by a calculated mean level of importance (weights) given by the subject matter experts by using a 7-point Likert scale. The final result is the quantity CPS (Cybersecurity Preparedness Scores) which can have values between 0 and 5. The CPS is the normalized sum (between the 5 groups of question according to the 5 NIST functions) of the products between the answers of the question (0 or 1) and the certain question weight.

Decision makers' perceived risk of cyber-attack

During the literature review in the study of Eilts, (whose instrument we have selected for the measuring and the comparative analysis of the cybersecurity posture), the risk is assessed by measuring the perceived impact and probability of threats. The 10 cyber-attack categories are defined according the classification types of cyber-attacks from (Ponemon Institute, 2018): General malware, Advanced malware/zero-day attack, Compromised/stolen devices, Cross-site scripting, Denial of services, Malicious insider, Phishing/social engineering, SQL injection, Web-based attack, other. Furthermore, the perceived likelihood, as well as, the perceived impact for these 10 categories (also formulated in the form of questions), on the 7-point Likert range is also measured. Then, for each of the 10 categories, the average value of the products (likelihood x impact) is represented in percent and given as DMPRCA (Decision makers' perceived risk of cyber-attack score).

Research and results

Previously described methodology have been utilized by using online survey instrument in order to make the quantitative assessment of the cybersecurity posture of small organizations in North Macedonia. We have selected a certain number of small organizations from different industries. The data collection was in the period between November 2022 and March 2023. The organizations were approached by phone, email and on site. Before the survey, the decisions makers' in these organizations were briefed that their answers and data will remain anonymous and only summarized and statistical results on national level will be published. In order to avoid unreliable results, the survey was conducted only when the research team was convinced that the decision makers' in the selected organizations were motivated to participate in the survey.

There are many different recommendations for the sample size for quantitative research in this and similar fields in order to have appropriate sample size justifications, ranging from 20 to 30 to 40 or more (Kothari 2004, Sauro & Lewis 2016, Lakens D. 2022). In this study the size of the sample was 20, which we consider as enough taking into consideration the nature of the study, the complicated process of performing the survey and the resource constrains. However, we have validated this sample size by statistical approach based on precision rate and confidence level with the relation n=(z×σ/e)^2, where n is the size of the sample size, z is the value of the standard variate equal to 1.96 for a 95% confidence level, σ is the standard deviation of the quantity CPS that was calculated to 1.08 and e is the standard error (e=z×σ/sqrt(n)=0.46). Thus, a value of n=20 was obtained. For the quantity DMPRCA also a value of n=20 was obtained, where the σ was calculated to 0.188 and e was calculated as 0.0824.

The data collected through the previously described instrument was quantitatively analyzed and values for CPS and DMPRCA were obtained. The values were positioned on the CyPRisT with the DMPRCA on the horizontal axis and the CPS on the vertical axis, Figure 4.

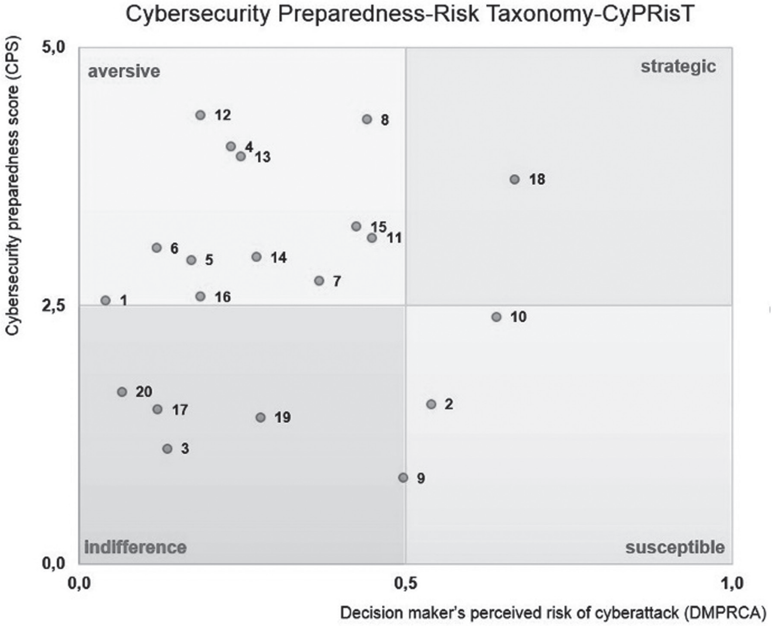


Figure 4. Position of the organizations in the CyPRisT

The summarized scores of the overall cybersecurity posture given by the quantities DMPRCA and CPS, on the sample of 20 organizations, are presented by the descriptive statistics in Table 1. This is done by calculating the central tendency measure, and the mean value, which is also accompanied by the standard deviation. The mean score of DMPRCA was 0.3, which suggests a low level of perceived risk of a cyber-attack. The mean score of CPS was 2.71 which indicates a middle range value of cybersecurity preparedness of the sample.

Quantity	N	Min	Max	Mean	Std. Dev.
DMPRCA	20	0.04	0.67	0.30	0.19
CPS	20	0.84	4.35	2.71	1.08

Table 1. Descriptive Statistics of DMPRCA and CPS in North Macedonia

Quantity	N	Min	Max	Mean	Std. Dev.
DMPRCA	216	0.02	0.85	0.28	0.16
CPS	216	0.14	4.47	2.29	1.06

Table 2. Descriptive Statistics of DMPRCA and CPS in USA, (Eilts 2020)

The data from Table 1 were compared with the data from (Eilts 2020), given in Table 2. The comparison between the position of the mean values in CyPRisT is presented in Figure 5, where the result obtained with the experimental research within this study in North Macedonia (Table 1) is marked with label "MK", and the result obtained in USA (table 2) is marked with "US".

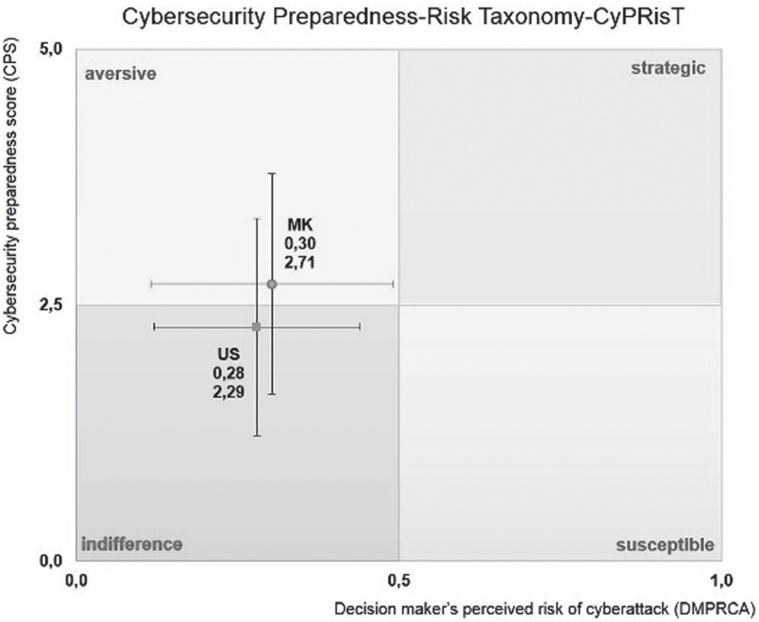


Figure 5. North Macedonia and USA CyPRisT score with standard deviations

These results were analyzed by using unequal variances t-test (Welch's t-test) for both quantities for DMPRCA and CPS, to compare the calculated means and to determine if statistically significant differences exist, taking into consideration that the researched populations, as well as the sample sizes and the variances, are different. Results of the test are presented in Table 3. The results indicated that statistically there were no significant differences between the means DMPRCA_{MK} and DMPRCA_{US}, as well as, between CPS_{MK} and $\mathrm{CPS}_{US.}$ However, we can observed an increase in both the CPSs and DMPRCA in North Macedonia that moved the position toward the 'aversive' quadrant of the CyPRisT.

Also, a qualitative comparison has been done with the results presented within (ENISA, 2021), where there are presented findings of the study which includes 249 SMEs from 25 European Member States. The low DMPRCA_{MK} is overlapping with the conclusion in (ENISA, 2021) that many SMEs do not realize the potential resultant cybersecurity risks posed to their business. Also, the middle range value of CPS_{MK} is overlapping with the conclusion in (ENISA, 2021) that SMEs appear to implement some of the basic cybersecurity measures mostly as part of their overall IT implementation or legal obligations.

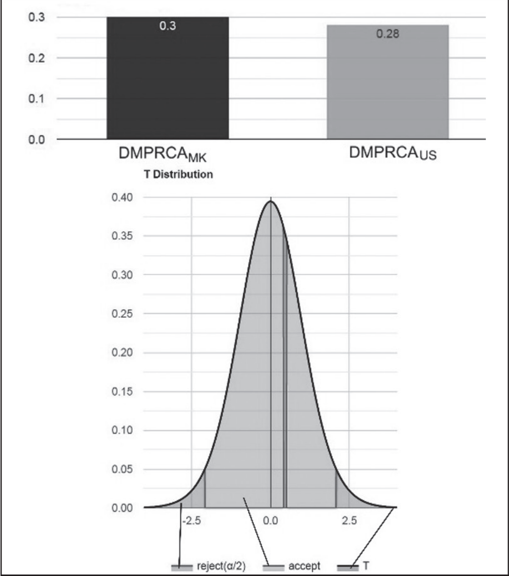
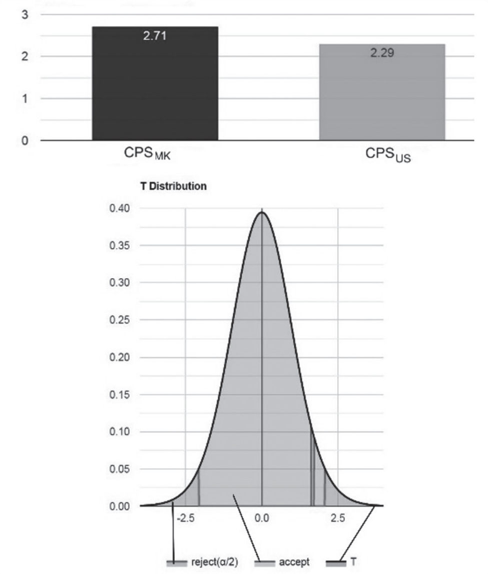
 	
α=0.05 df=21.5688 (two-tailed) Since p-value > α, H_0 cannot be rejected p-value = 0.6529 T = 0.456 $\overline{\text{DMPRCA}_{\text{MK}}} - \overline{\text{DMPRCA}_{\text{USA}}}$= 0.02 standard dev. of the difference, S' = 0.0439 The observed effect size d is small, 0.12	α=0.05 df=22.5247 (two-tailed) Since p-value > α, H_0 cannot be rejected p-value = 0.1095 T = 1.6664 $\overline{\text{CPS}_{\text{MK}}} - \overline{\text{CPS}_{\text{USA}}}$= 0.42 standard dev. of the difference, S' = 0.252 The observed effect size d is small, 0.4

Table 3. Two sample t-test (Welch) results, using T distribution

Conclusions

This study addresses research questions which a relevant and significant in the field of security of IS. It presents new findings which includes quantitative measurement of the current cyber security posture in North Macedonia, as well as, quantitative and qualitative comparison of these results with similar ones gained in studies in the EU and the USA.

This study showed that less than a quarter of small organizations in North Macedonia are potentially indifferent toward cybersecurity, which compared with the USA is better, where more than half of the SMEs were positioned in this group. Also, the results showed that, just a few of the organizations were estimated as having risk-seeking cybersecurity postures, which is overlapping with the findings in the studies in the USA and the EU. Most of the organizations in North Macedonia were positioned as loss aversive. Loss aversion appears to be the principle driver for decision biases. This suggest that existing regulations, especially in the banking and IT sector are giving results, but the decision makers are not enough focused on managing the cyber threats. The findings also barely noted the existing of a posture where there is strategic balance between understanding cyber risk and implementing the security actions to deal with cyber threats, which is the same finding as in the studies in the EU and the USA.

One very practical implication which arises from this study is that there is necessity of further development of programs that can help small organizations to improve their cybersecurity posture. Most important would be developing the awareness of decision makers to mitigate the cybersecurity risks in parallel with the existing focus on their primary activities. This will contribute to small organizations becoming more risk aversive.

Recommendations for future research

During the implementation of this study within its limitations, we experienced a feeling that we just scratched the surface of the topic, so herein we can give some of the many questions which we find important for future research:

- Enlarging the number of the sample – number of researched organizations;
- Further statistical analysis in terms of organizations' demographic data of industry, number of employees (size), years in operation, annual revenue, and IT budget;
- Analysis of CPS and DMPRCA when compared by industry, number of employees, and IT budget;
- Analysis of DMPRCA in terms of perceived likelihood of the cyber-attack by attack vectors;
- Analysis of CPS in terms of perceived impact of the cyber-attack by attack vectors.

REFERENCES:

Bazerman, M. H. (1984). The relevance of Kahneman and Tversky's concept of framing to organizational behavior. Journal of Management, 10(3), 333-343.

DCMS (2020). UK Department for Digital, Culture, Media and Sport: Cyber Security Breaches Survey 2020: Statistical Release.

EC (2021). European Commission: User guide to the SME Definition.

Eilts, D. (2020). An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses, Doctoral dissertation, College of Computing and Engineering, Nova Southeastern University.

ENISA (2021). European Union Agency for Cybersecurity: Cybersecurity for SMEs, Challenges and Recommendations.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. Information Management & Computer Security, 13(4), 297-310.

Kothari C. R. (2004) Research Methodology, Methods & Techniques, New Age International Publishers.

Lakens D. (2022). Sample Size Justification. Collabra: Psychology 8(1):33267.

Tversky, A., & Kahneman, D. (1991). Loss aversion in riskless choice: A reference dependent model. The Quarterly Journal of Economics, 106(4), 1039-1061.

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. Journal of Risk and uncertainty, 5(4), 297-323.

NIST (2018) National Institute of Standards and Technology: Cybersecurity framework, Retrieved from https://www.nist.gov/cyberframework

Ponemon Institute (2018). State of cybersecurity in small & medium-sized businesses (SMB). Retrieved from

https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

Sauro j., Lewis J. (2016). Quantifying the User Experience: Practical Statistics for User Research. Elsevier.

Original scientific article
UDK 613.2:614.31:[355.1(497.7)
UDK 631.147:546.3:[355.1(497.7)

FOOD SAFETY AND RISK ANALYSIS THROUGH EXAMINATION OF TOXIC METALS IN FOOD PRODUCTS

Nadica TODOROVSKA[1]
Ljupcho SHOSHOLOVSKI[2]

Abstract: *Nutrition is one of the most important elements that affect human health, work ability and length of life. That is why it is necessary that the food products which are consumed daily are of high quality, but also safe, that is, do not contain substances harmful to the body. Food safety in all branches of food industry (production, processing, packaging, storage, transport and sale) is of increasing importance. International quality and health conformity standards establish norms for the chemical composition of food products and define the minimum and maximum amounts of certain parameters. Each state applies the prescribed standards through the adoption of appropriate laws and regulations. Heavy metals in food can be present as environmental contaminants or as residues from treatments used at all stages during production. If they are present in food products above the maximum allowable values, they can have a toxic effect. In this paper, using the AAS technique, the metals lead and cadmium were analysed in 37 food products that are used in the collective diet of the members of the North Macedonia Army. The results showed that the obtained parameters correspond to the valid regulations for the examined metals and that they are safe to use.*

Key words: *food products, food safety, standards, AAS, lead, cadmium.*

Introduction

Food safety is one of the basic interests of the modern human. The products used in daily diet are called livelihood or food products. According to their origin, they are divided into animal, vegetable, and inorganic products, and according to their role in the body, into energy, building, and protective products. They contain nutrients, as well as other substances that are added for preservation, repair of their organoleptic properties such as taste, smell, appearance, etc. In order to satisfy the increased demand and food consumption, chemicalization is carried out in agriculture, which, in addition to the increasing pollution of nature and the environment, poses a danger to human health and the survival of life on earth in general.

The quality regulations determine the norms regarding the chemical composition of the products, as well as other qualitative properties characteristic of the respective food product. Regarding the chemical composition, the minimum quantities of the substances that the food must contain, the maximum quantities of those substances that it may contain, as well as the substances that must not be present are defined. The tendency in all developed countries in the

[1] The author holds PhD, Military Medical Centre Skopje

[2] The author is Professor at the Military Academy “General Mihailo Apostolski”, Skopje

world is to recognize certain risks and reduce them to the lowest possible level by applying modern scientific methods.

Due to the increasing demands of consumers, the increased responsibility of producers and commerce, globalization and the tightening of legal obligations, the need to develop standards for ensuring food quality and safety is emphasized. These standards refer both to the quality and to the hygienic conformity of food products that directly affect consumer health.

Health safety control is a very important measure that ensures that food products meet the hygienic requirements for the content of microorganisms, parasites, chemical and other foreign substances. The risk to the consumer health can be effectively reduced by identifying the points of risk in food production, and therefore the international codes and standards including GlobalGAP, ISO 22000 and Codex Alimentarius are characterized with a preventative approach.

GLOBAL GAP (Good Agricultural Practice) is put into the function of consumer protection with the motto that everyone has the right to quality, and first and foremost, safe food. The overall system for the control of food production in the European Union (a possibility for food monitoring from field to table) has significantly changed with the introduction of new and stricter legal regulations.

ISO 22000:2005 is a food safety system and it is the first international standard that specifies the requirements for a food safety management system so that every organization in the food chain (primary producers, processors, transport and storage, retailers, as well as manufacturers of equipment, packaging, cleaning agents, additives, food ingredients, etc.) must demonstrate the ability to recognize and control critical points of hazard and ensure that the product is safe for consumption.

Codex Alimentarius is a collection of internationally recognized standards, rules and practices, guidelines and recommendations relating to food production and safety. The Codex Alimentarius Commission (CAC) adopts standards and recommendations for their use based on chemical specifications and health safety assessment through its committee. The purpose of the Commission is to protect the health of consumers, ensuring good practice in international food trade by prescribing rules for the regulation of agriculture and the food industry and complete control of food, regardless of whether it is processed, semi-processed or raw. EU member states are obliged to incorporate those standards and recommendations into their legislation.

Food safety in our country is regulated by the Law on Food Safety published in the Official Gazette of the Republic of Macedonia [1], and the prescribed international standards are selectively applied through appropriate regulations [2].

Food safety is defined as an acceptable level of consumer protection, where the food does not pose a risk to their health, if it is prepared and consumed in the intended way for its use. In order to ensure food safety and security, it is necessary that the level of hazard be below the maximum allowable concentrations determined by international and national legislation.

By applying food safety methods, the risk for the individual using the respective food is not determined, but the safety level of the population is identified. One of the most important tools is the risk analysis methodology. Risk analysis is a process consisting of three interrelated components: risk assessment, risk management and risk communication, and is carried out in order to achieve a high level of protection of the life and health of consumers.

Risk assessment is a science-based process that is founded on available scientific evidence and is conducted in an independent, objective and transparent manner. It consists of four stages: hazard identification, hazard characterization, exposure assessment, and risk characterization.

Three methods are used for the exposure assessment (qualitative and quantitative assessment of probable intake of the agent through food and other sources or total daily intake of the chemical substance in the human body EDI – Estimated Daily Intake [3]): examination of dietary intake through daily meals, examination of exposure per capita and results of the consumer basket analysis (through individually selected food products) and total food intake. The third method is the subject of the experimental part of this paper.

Food contamination with toxic elements, such as heavy metals, is a serious problem, starting from its production (contaminated land, water and air), through processing, packaging and storage, to preparation for use. The salts of the elements normally enter in the natural composition of the environment, and through it also into many products. Those concentrations are minimal and harmless. However, industry, traffic, the irrational use of artificial fertilizers and pesticides pollute the ecosystems with additional amounts of contaminants which, through products of plant and animal origin, are introduced into the human body. Those pollutants are resorbed in the digestive tract and cause damage at the level of body organs and tissues. On the other hand, some toxic elements, such as lead and cadmium exhibit toxic properties even in relatively low concentrations and have the ability to gradually accumulate in tissues [4].

Lead is the most abundant of all heavy metals in nature. The human can be exposed through: sources of industrial origin, the metal industry, industrial waste, tetraethyl-lead in gasoline, lead-based paints, through the packaging of food (cans) containing lead and others. Lead is deposited in the bones, liver, kidneys and soft tissues. Lead poisoning adversely affects the brain and nervous system function, reduces the degree of intelligence, power of observation and memorization. In the most severe cases, it leads to death.

Cadmium in nature is usually present in the soil, but in food it also comes from the use of some fertilizers. It can be found in cereals, potatoes and other root vegetables, but also in animal internal organs. It is deposited in the liver, kidneys and bones. It causes anemia, bone deformation, elevated blood pressure, damage to the heart and kidneys, and has a carcinogenic effect [5].

Material and methods

Atomic absorption spectrometry is an analytical technique that enables the quantitative determination of about 70 elements (metals and metalloids) in low concentrations. It is applied in all areas of analytical chemistry practice. It is an economical, easily adaptable technique and enables the solution of a large number of problems that used to require long-lasting procedures or the use of expensive and inaccessible equipment. It is one of the most significant applicable methods for the analysis of the elemental composition of various materials and samples.

For quantitative determination of the presence of the examined elements in the samples, the following instruments were used:

-Varian Atomic Absorption Spectrometer, model SpectrAA 220Z, with Zeeman corrector, GTA 100 graphite furnace and auto sampler;

-Sartorius CP 3245 scale;

- Adrona Crystal E deionized water device.

In the process of electrothermal atomization, two types of graphite furnaces were used: pyrolytic coated tubes and tubes with a centrally fixed L'vov platform.

Hollow cathode lamps were used as a source of radiation. They are optimized about 15 minutes before starting the analyses.

In order to achieve greater sensitivity and better precision, before starting the analysis, optimal instrumental conditions are determined for each element individually.

The methods and procedures applied in the experimental work are determined by the regulations in the field of food testing, by the operating manuals of the corresponding instruments recommended by the manufacturer, as well as by the methods published in the works resulting from the previous scientific research or taken from papers cited in the literature.

The calibration method is applied on a sample to which a standard additive has been previously added. The calibration samples were prepared in duplicates and with concentrations at three points covering the measurement range of each element respectively.

The food product samples, immediately upon their reception in the laboratory, are prepared for analysis and are converted into a solution by wet decomposition with an oxidizing agent at a suitable temperature [6].

The analytical methods correspond to the methodology for determining the concentration of toxic elements in food products [7].

In order to determine the concentrations of lead and cadmium, basic standard solutions of: cadmium nitrate Cd(NO3)2 and lead (II) nitrate Pb(NO3)2 were used, with a mass concentration of 1 g/L of cadmium and lead, respectively, manufactured by Merck, Germany.

The working standards are prepared immediately before use by dissolving the basic standard with ISO3696 Grade I deionized water (conductivity to 0.1 microS/cm).

Nitric acid, Tracepur®, 69% (m/V) produced by Merck, Germany was used as an oxidizing agent.

Three samples from each of the different units of 37 food products that are in daily use within the collective diet of the Army members of North Macedonia were tested.

Results and discussion

In order to implement food safety methods in our country, the tool for risk analysis methodology through exposure assessment by analysing the amount of heavy metals (lead and cadmium) in food products from the consumer basket (through individually selected food products) was applied to achieve a high level of protection of the life and health of consumers, users of collective nutrition in the Army of North Macedonia.

As part of the regular work of the laboratory at the Department of Preventive Health Care in the Military Medical Centre Skopje, the uncertainty of the methods is calculated on the measurements of the middle point of the calibration curves. The methods have been validated by the method added found (spiked samples) for several samples [8].

Table 1 shows the mean values of the obtained results for each product from the consumer basket.

Examined food products	Cd mcg/kg	Pb mcg/kg
Rice	25.67	47.67
Flour	9.00	69.33
Bread	6.67	36.00
Pasta	2.67	30.00
Tea biscuit	1.33	53.00
Beans	16.67	15.33
Carrot	1.33	14.67
Potato	44.67	5.00
Onion	8.67	45.00
Cabbage	3.33	12.67
Spinach (fresh)	7.00	253.33
Tomato puree	43.33	696.67
Champignon mushrooms	2.67	115.00
Ground paprika	17.03	466.67
Black pepper	0.10	148.33
Parsley	22.00	286.67
Spice mix	43.33	696.67
Cocoa powder	0.10	108.00
Salt	0.40	28.33
Chicken soup	8.00	158.33
Apple	3.33	14.00
Orange juice	5.33	32.00
Plum compote	0.10	36.00
Chicken	16.33	92.00
Pork sausage	79.33	145.00
Beef sausage	12.00	216.33
Chicken eggs	1.67	112.67
Mayonnaise	1.37	49.33
Canned sardines	5.67	131.33
Sterilized milk 3.2% m.f.	2.37	16.33
Yoghurt	0.73	12.67
White cheese	0.73	64.67
Yellow cheese	0.10	62.00
Butter	0.73	67.33
Sunflower oil	5.00	27.33
Mustard	9.33	80.67
Honey	4.00	14.00

Table 1. Obtained results from the examination of the amount of lead and cadmium in samples of certain food products from the consumer basket used for collective nutrition in the Army of North Macedonia.

In the food samples, the amount of cadmium and lead was determined, which is below the limits of the maximum allowable concentrations MAC, determined by the current legal regulation [1, 2]. All are considered correct and safe to use in terms of the parameters tested.

The highest amounts of cadmium were measured in the group of vegetables, followed by food products in the group of grain and grain products. The lowest amounts of cadmium were measured in foods in the group of eggs and products. The highest amounts of lead were measured in the group of meat and products, while the lowest amounts were measured in foods in the group of fats and oils.

Conclusion

"Everything is poisonous and nothing is poisonous, it is all a matter of dose." Claude Bernard 1813 - 1878

The measured amounts of heavy (toxic) metals of interest for this paper, lead and cadmium, in the examined food products were below the maximum allowable concentrations according to the current legislation [1, 2].

In the implementation of food safety methods within the framework of collective nutrition in the Army of North Macedonia, the tool: methodology for risk analysis through exposure assessment by analysing the amount of heavy metals (lead and cadmium) in food products from the consumer basket (through individually selected food products), showed that all the tested foods were correct and safe for use in relation to the tested elements.

The results of this research point to the necessity of regular examination of products intended for collective consumption of the Army members of North Macedonia and timely response and removal of those measured with higher amounts of contaminants than the maximum allowable according to the current legislation. With this type of examination, an important step is taken towards achieving a high level of protection of consumer life and health, since all food products are purchased from the regular market of the country.

In order to facilitate the production and provision of high-quality and safe food, international standard norms for its hygienic conformity and quality are being created. For the application of those norms in each country, it is necessary to develop adequate methods and criteria. The methods and procedures for determining the prescribed properties (qualitative and quantitative) should follow the contemporary scientific and professional technological achievements. For this purpose, it is necessary at the national level to develop well the established international norms and apply them for the health conformity and quality of food distinctive to each country, and to adequately and precisely develop the criteria and methods for examination of food products, especially for examination of the quality of some product groups. Hence, the application of different test methods in the analysis and superanalysis of food products and the possible obtaining of different results that may lead to confusion and unwanted consequences will be avoided.

REFERENCES:

Official Gazette of RM, Law on Food Safety Of. G. RM No. 157/2010

Official Gazette of RM, Rulebook on General Requirements for Food Safety Of. G. RM No. 118/2005; Rulebook on General Requirements for Rood Safety Regarding Maximum Levels of Individual Components, Of. G. RM no. 102/2013 and Rulebook for Amendments Of. G. RM no. 175/2018

FAO/WHO Trace Elements in Human Nutrition and Health. World Health Organization. Geneva, Switzerland. 1996

Beckett W. S, Nordberg G. F, Clarkson T. W. Routes of exposure, dose and metabolism of metals. Elsevier Amsterdam-Tokyo. 2007: 39-76.

Тошовић С., Основи екотоксикологије; Висока здравствено-санитарна школа струковних студија ‘’Висан’’; Београд, април 2009. /Tosovic S., Basics of Ecotoxicology; Higher health and sanitary school of professional studies ‘Visan’; Belgrade, April 2009.

Subramanian K. S. Determination of metals in biofluids and tissues: sample preparation methods for atomic spectroscopic techniques. Spectrochimica Acta Part B: Atomic Spectroscopy. 1996: 51 (3): 291-319.

Alzahrani et al., 2016). Alzahrani H. R, Kumakli H, Ampiah E, Mehari T, Thornton A. J, Babyak C. M, Fakayode S. O. Determination of macro, essential trace elements, toxic heavy metal concentrations, crude oil extracts and ash composition from Saudi Arabian fruits and vegetables having medicinal values. Arabian J Chem. 2016: 10 (7): 906-13.

Ajai A. I, Ochigbo S. S, Abdullahi Z, Anigboro P. I. Determination of Trace Metals and Essential Minerals in Selected Fruit Juices in Minna, Nigeria. Int J Food Sci. 2014: 1-5.

Scientific article
UDK 355.02:327(470+571:477)"2022/2023"
UDK 355.48(470+571:477)"2022/2023"

THE RUSSIA - UKRAINE WAR IMPLICATIONS AND CHANGES IN WORLD POLICY

Igor GJORESKI[1]

Abstract: *The year 2022 began as the year with the challenge of providing resources in support of the accelerated post-COVID 19 economic development. However, at the end of February 2022, a precedent occurred in the form of Russia's unjustified aggression against Ukraine that directly challenged security, peace and stability on European soil. For the first time since World War II, the states have faced a conventional threat that threatened to involve Europe and the world into a new war on a wider scale. In the first days of the aggression, the quick reaction of the Ukrainian people was crucial. This reaction contributed to slowing down the advance of the Russian forces on the battlefield and the military action did not proceed according to the dynamics planned by Moscow. The success of the Ukrainian Army gave the democracies enough time to organize and deliver humanitarian aid and other support in equipment and armaments to help Ukraine fight Putin's aggression. The challenges to the states were reflected through the slowed down economic growth, uncontrolled rising energy and food price, through the lack of raw materials for production, lack of food, etc., which also encouraged increased inflation and a decline of the living standard of the citizens. The war accelerated the process of diversification of the energy supply and reduced the dependence on Russian gas and oil of the European countries. In addition, every war is followed by refugees, accelerated migration and internally displaced persons in the affected countries. In this regard, the EU has activated mechanisms to deal with mass migration and opened its borders for the reception of refugees from Ukraine and their integration. Every war is followed by a large number of victims on both sides and destroyed infrastructure on the ground. This war will be remembered as a technology advanced war in which both sides actively use emerging and destructive technologies on the battlefield. The results on the ground from the use of these technologies is overwhelming and with catastrophic destruction.*

Key words: *War, emerging technologies, post conflict reconstruction, migration, critical infrastructure.*

Introduction

The unjustified Putin's aggression against Ukraine was the major event of 2022. At the beginning, both Moscow and the West expected that the war will finish very quickly and the Russian forces would achieve a quick victory over Ukraine. However, the reality proved rather different. After the initial success in occupying some northern, eastern, and southern regions of Ukraine, the troops of the Russian Federation were forced to retreat from most of their Ukrainian positions. Still, more than one year of fighting, war crimes, mass migration of

[1] Assoc. Prof. Dr.sc, Ministry of Defense of the Republic of North Macedonia

the Ukrainian population and a serious contraction of the Ukrainian economy, the war goes on (Minakov et all, 2023).

The consequences of the war in Ukraine are reflected on politics, economy, food supply, lack of energy, migrations and in other segments of human life. Such implications have caused a re-actualization of power politics, an increase in food and energy prices, disruption of trade relations, migrations and etc. which have an impact on increased inflation and deterioration of the quality of life.

The implications of Russia's aggression against Ukraine continue to create serious headwinds for global economy. The global economy is expected to slow further in the upcoming period, as the massive and historic energy shock triggered by Russia's war of aggression against Ukraine continues to spur inflationary pressures, sapping confidence and household purchasing power and increasing risk worldwide.

The outbreak of war in Ukraine has impacted many spheres of political, economic and social life. It includes the extraordinary prelude on migration flow in neighboring and other European countries. By far, the UN estimates more than several millions Ukrainians finding refuge in some of the European countries.

In general, the consequences of the war are devastating in all aspects and for all of us. Having in mind the situation on the ground -the battlefield, the Russia-Ukraine war is the most technologically advanced war that humanity has ever seen thus far. Numerous predictions have been made about how new technologies would feature and fare on a battlefield of the future. So far, the estimates are that around 100,000 Russian and more than 10,000 Ukrainian service personnel have been killed (NBC News, 2022). According to OHCHR reports, more than 7,000 Ukrainian civilians have died in the last year as a result of the war, including more than 460 children (OHCHR, 2023). The estimation does not include the devastating effects to critical and other infrastructure.

In the Russia – Ukraine war one thing has become clear. There are many predictions and scenarios how this war will end. However, there is only one option for western democracy – Putin's Agenda must be defeated and Ukraine must win the war. The outcomes of the war are not clearly predictable. Many leaders of the free world agreed that this is not a war of Russia's people but, it is a war of Putin's authoritarian regime and its elite against Ukraine. It is not so clear how the war will evolve on the ground this year. This is a bit complicated because of Putin's nuclear rhetoric and its actions close to nuclear power plants.

Outcomes of the war

At the moment it is almost unfeasible to claim that we are considering all aspects and the reflections of the global shock provoked by Putin's decision to launch a full-scale re-invasion of Ukraine one year ago. It will take time until we become consciously aware of the full spectrum of changes and the main outcomes of the war so that we can predict with certainty the precise evolution of situation in the 2023. However, even now we can envisage three or more general and rather serious implications for the countries and the world.

As Chatham House experts examine the shifts and assess the results of the Russian war on Ukraine only a week ago, we should emphasize that what we should expected are provisional changes in geopolitical alliances and security, energy and supply chain changes and certainly additional economy and banking adjustments. Another question is whether these changes are likely to be long-lasting.

It seems that STRAFORT 100 years forecast can have a significant impact on reality with the new geostrategic projections. It means that there will be a realignment of a major group of nations being supportive to Ukraine, small not equivocal supporters of Russia and a group of equidistance, but still influential from aside, and they will project the way of the new geopolitical reality to come.

It appears that many of Russia's neighbors had been correct in their analysis of the threat posed by Moscow's regional ambitions. There is little on the horizon that could alter this path. However, with its gas, Russia's political influence in Europe wanes (Jenkins, 2023), as well as Moscow's isolation from Europe (Minakov et all, 2023). Also, it is difficult to say whether the West will restore its good "postwar" relations with Russia.

As a consequence, as Russian influence fades, there will be a new opportunity for a race of the new regional players in Europe as George Friedman predicts. It means by the end of the year, as any war is rounded up with the peace accord for a hypothetically frozen conflict, there will be end of hostilities, division and negotiations on how to proceed although there will be no more business as usual, as some people want to say (Freedman, 2010).

While the pandemic highlighted the vulnerabilities of just-in-time supply chains, the economic fallout from the war in Ukraine has underlined the additional risks in such a system. Globalization is not dead, and world manufacturing and commerce will continue. But the new geo-political environment will affect the future corporate decision-making. Cost savings will be more closely scrutinized against risk. De-globalization means increased prices, at least in the short run, adding to inflationary pressures (Jenkins, 2023).

The war speeds up the implementation of many 'dormant' processes in the both NATO and the EU. I can freely say that the war in Ukraine has bolstered Europe's commitment to increase defence spending. In 2023 two/thirds of the NATO members achieved the Defence Investment Pledge for 2014 Wales Summit of at least 2% of GDP to invest in defence, out of which at least 20% is to be allocated for procurement of new major equipment and R&D, wherefrom major defence manufacturers will benefit (Trismpioti, 2023). This trend has already been reflected in the surge of their share prices. Whether manufacturers can ramp up to meet the demands remains a question.

In fact, the war has accelerated the actions which were 'unthinkable' before the war, Russia's invasion has strengthened NATO's deterrence posture and increased its forward and vigilance presence in Eastern Europe, Finland and Sweden, two countries which have until now shunned NATO membership to avoid antagonizing Russia, are also set to join the alliance in a historic shift and crucially, US support for NATO and security in Europe also appears cemented with bipartisan support at home. The "success" in Ukraine will strengthen the alliance (Jenkins, 2023a). NATO members invest a lot in line to increase the defence capabilities of the alliance, in order to strength their posture against Russia.

The current situation virtually re-creates the Cold War division of the global level at many sectors, and, Russia is at a greater disadvantage (Jenkins, 2023), since it no longer operates in the larger space of the Soviet bloc (the Council for Mutual Economic Assistance—COMECON) whose one-time members are now members of the EU and NATO.

Economic Impacts of the War

The impact on the part of the global economy, banking and the supply chain has also increased. In conditions of still complicated supply chains, and a gradual post-pandemic recovery in demand, pressures on prices were felt, which escalated with the war in Ukraine. This additionally reduced the supply and increased the uncertainty, so all this reflected on energy and food with additional implications from the introduced sanctions against Russia. Such situations were manifested primarily in an energy crisis that spilled over into the general level of prices through the growth of production costs and caused a crisis in the cost of living.

Let us go step by step with the impact of the war in Ukraine on the economy and speak a little bit about the impact on the economy closely related to energy dependence, food shortage and growing inflation.

Going back to the beginning, 2022 was predicted as a recovery year with an estimation of 5% economic growth. Two months later, the war in Ukraine was a “massive and historic energy shock” (Jenkins 2003) to the markets. The “shock” was one of the main factors that slowed economic growth in 2022 to just 3.1 percent. The aggression on Ukraine by Russia has had the greatest impact on Europe’s economy, where the growth in 2023 is projected to be just 0.3 percent (Jenkins 2003).

One of the “secret” weapons in the hand of Putin was Europe’s energy dependence by Russian gas and oil. In the first days of the Russian aggression, the prices of oil and gas, and the most important Russian exports, rose significantly. The price of gas more than doubled and oil prices rose above US$125 per barrel (KPMG 2022). Exports of oil and gas were Russia’s primary economic interaction with the West. These exports are unlikely to be restored to pre-invasion levels. Europe has faced a leak of energy diversification supply. According to Moscow, in the first three months of the war Russia increased its finance by energy export of gas and oil for more than $100 billion. Moscow’s energy export revenue reached $338 billion in 2022, more than a third from $244 billion in 2021 (Radio Free Europe/ Radio Liberty 2022). It is a huge amount of money. However, these days Europe is almost energy independent from Putin’s gas and oil because of the EU’s decision to reduce the price of oil and gas imported from Russia. This decision causes a significant decline in the export of Russian gas to Europe, reduces Russian state revenue, which also disrupts the cash flow that supports the Russian political leverage.

Also, the war caused food shortage across the globe. Russia’s 2022 invasion disrupted key markets and supply chains for crops and fertilizers that significantly affect global food security (The World Bank 2023 p4.). Still, Russia remains the world's largest exporter of wheat and forestry products, and a source of strategic resources such as nickel, cobalt, and platinum (Jenkins 2023). Figures from the UN Food and Agriculture Organization (FAO) show that in 2020 Russia accounted for about 11 % of the global wheat production and 19 % of the global wheat exports (making Russia the world's largest wheat exporter that year). In addition, Russia is a globally significant exporter of barley, sunflower oil and sunflower seeds (BOFIT 2022).

Ukraine, is the second biggest exporter of wheat in the world, and many countries from the third world were faced by a food shortage. Ukrainian exports of corn, wheat, and barley for January through November 2022 were 22 percent below 2021 levels. Ukrainian grain exports to the developing countries remain below pre-war levels. Ukrainian wheat exports to the least developed countries have more than doubled since the start of the war, but export volumes in 2022 were 1.6 million tonnes below those of 2021 (The World Bank 2023 p9.). Many manufactures were dependent on the resources produced in both countries. The consequence was a slowed down production. These are only some of the factors that injected the growing inflation and caused a decline in the living standards. Regardless of the outcome of the war, Western companies will remain reluctant to return to Russia, or invest in it in the future. The risks are simply too high.

In short, the war in Ukraine adversely affects inflation, raising it to historic levels and adversely affecting economic growth with risks of recession and great uncertainty. We are witnesses that Europe, with US support, made multiple steps and quickly built mechanisms to figure out the above-stated challenges. These days, the prices of the oil and gas are stable and much lower than six months ago, the situation with food is stable, and the economic "shocks" of the war are almost in the past.

Globally, the high inflation encouraged a faster tightening of monetary policies and a slow process of fiscal consolidation with additional borrowing by countries after the primary borrowing due to the pandemic. The reflection of the central banks acted in synchronization, which affected the demand and economic growth by increasing interest rates, and thus the cost of loans and investment intentions. Therefore, in the short term, it is realistic to expect weaker economic growth globally, especially in the Eurozone, but also around the world. Over time, fiscal policies will have to consolidate whether this is done by reducing transfers and public consumption and raising taxes or, as has often happened in the past, by cutting public investment. The government policies usually redirect investment to where it is needed in order to achieve non-inflationary growth (Lagarde 2022).

However, after 2023, economic consolidation and utilization of the new opportunities that will be brought about with the reconstruction of the conflict-devastated areas are expected.

The devastation caused by the war in Ukraine is huge in all aspects. It will require post conflict reconstruction, but it depends on how the war will end. There is one option, Ukraine must win the war. However, rebuilding Ukraine may be more financially difficult than conducting the war itself. The country has already suffered levels of damage not seen in Europe since World War II, and it took 20 to 30 years for Germany and the United Kingdom to rebuild after the war. Estimates of how much it will cost to rebuild the country vary (Jenkins 2023). The current estimation of the World Bank is that the cost of rebuilding Ukraine would be more than $410 billion, (The World Bank 2022) a number that is larger than Ukraine's pre-invasion GDP and three-times greater than all the military, humanitarian, and financial assistance commitments to Ukraine since the start of the war, and is certainly much higher now. According to the Ukrainian President Volodymyr Zelenskyy "the price tag (for post conflict reconstruction) would likely top $1 trillion and increases every day the fighting continues" (Garver 2023).

So far, one thisn is clear. It is yet not certain how the war in Ukraine may evolve in 2023. Despite heavy casualties, neither side is visibly falling apart or appears ready to back down. Both sides are digging in, but as the spring mud dries and the ground hardens, new offensives can be expected. Whatever happens and how the war evolves in the coming months and even years, everyone needs to be prepared to accept the consequences. Also, the politically sensitive what-if questions cannot be ignored. The final outcomes of the war depend much more on the Western support to Ukraine in all aspects, including modern platforms.

The Russia – Ukraine War and Historic Migration Flows

The war initiated by Russia against Ukraine in February 2022 generated a historic outflow of people, largely women and children or refugee migration in Europe since World War II. This migrant crisis is quite different than the Syrian and other Middle Eastern or West Africa's migration flows. Around 8.2 million people have been displaced from Ukraine into Europe (Botelho, and Hägele 2023) according to data assembled by UNHCR. This corresponds to around 20% of the total Ukrainian population. Roughly 19.7 million people left Ukraine UNHCR (2023), while 11.2 million (CReAM 2023) have since returned to the country. This number of immigrants will significantly influence the demography of the recipient countries, especially if they have a small population. A number of European countries already host a significant Ukrainian diaspora. These are migrant workers who arrived starting in the 90s, in a continuous flow. This time around, the fate of the people of Ukraine seems to be of much greater concern than the impact of the refugee influx on European societies.

Notwithstanding, the unprecedented inflow of war refugees clearly raises questions about future developments and challenges related to the presence of Ukrainian citizens abroad. Amplified by the war, this phenomenon is in addition to the former geographic factors and the long-lasting tradition of (labor) migration. So far, the EU stands in full solidarity with Ukraine and its people. In response to Russia's aggression, the EU has shown unity and strength and has provided Ukraine with coordinated humanitarian, political, financial and material support.

Despite being subject to great uncertainty and regardless of the developments on the front line, we have to reckon with the fact that the number of immigrants from Ukraine will continue to be significantly higher in the months before and maybe some months after the ceasefire and forced peace. In addition, we should not forget the human rights abuse by forced transfers of unaccompanied children to Russian occupied territory which makes the situation with migrations and refugees even more complex.

All of the afore-stated poses certain challenges for the public services and public institutions in the recipient countries. One of the outcomes in some of the neighboring countries, is that the influx of war refugees from Ukraine changed the status of the recipient countries from typical emigration to immigration countries, without going through an intermediate phase.

Despite the positive medium-term effects, the presence of migrants causes some short-term challenges. On the one hand, Ukrainian migrants drove a short-term surge in retail trade and private consumption during 2022, particularly in Poland and Estonia. Furthermore, if migrants become integrated, they will also boost the labour force in the recipient countries and contribute positively to the output in the medium to long run. This will have a positive impact on economic growth, and will increase the challenges for public finances of the recipient countries. On the other hand, in particular, the expenditures of Ukrainian migrants were an additional factor for the high growth rates of inflation in the EU, where it was already decade-high on the back of the surge in energy prices (Duszczyk and Kaczmarczyk 2022).

For countries hosting refugees there are pressing questions: will most of those who have fled Ukraine return, or will families eventually be reunited abroad, possibly implying an even greater inflow of Ukrainians into Europe and elsewhere when the war is over?

A more reliant outcome depends on the scenario forecast for the length of the war and the conflict activities in Ukraine. In the first scenario (long continuous war, mostly on a regional level), we could expect a continuation of the conflict and an additional migration flow. In the second scenario (a quick and lasting peace), one should assume a quick (by autumn) conclusion of peace, which will stabilize the situation in the short run and will also bring relatively favorable conditions for the return of refugees which is not an easier option to organize and sustain. The third scenario is – at the level of assumptions – similar to the previous one, but we assume that the war will also lead to greater destruction in western Ukraine, whereas a peace agreement will be signed earlier than assumed in the first scenario. Scenarios two and three should assume significant investment to rebuild the damaged infrastructure, financed either by international aid or reparations (Duszczyk and Kaczmarczyk 2022).

Regardless which scenario takes place, it will materialize long-term stays of war refugees in recipient countries, generate numerous challenges in the field of social services, which must be prepared to serve a larger number of people in the longer term.

One of the key questions arising from the migration flow is closely related to the will of the migrants to return to Ukraine. According to estimationa, once the war is over, more than 2 decades will be necessary to reconstruct the Ukrainian infrastructure and economy. During this period, many Ukrainians will be integrated in the hosting countries, and it is unlikely that they will return to Ukraine. Also, this migration flow is more than welcomed for the EU countries which are in high demand of labour force. Job market mismatch is a defining characteristic of large refugee inflows, even in relatively healthy economies. The vast majority of Ukrainian refugees are women and children and many women compete for a small number of jobs that can accommodate childcare needs. The OECD estimated that Ukrainian refugees will increase the EU labour force by 0.5 percent by the end of 2023 (Botelho, and Hägele 2023). Personally, I think that this migration flow is a question which needs more political debate for the future policy of migration flows from third countries and countries affected by a variety of different types of conflicts.

Migration forecasting is a second tool to assist smart solution for contingency planning to deal with migrations and refugees. Forecasting enables attempts to predict future migration flows and trends using, traditionally, quantitative modelling methods with a medium and long-term horizon. This approach statistically models future migration trends based on quantitative data from the past. In addition, foresight as an approach tends to use qualitative scenario methods to describe future migration flows and trends as qualitative narratives about the future of migration that examine possible structural changes and their consequences for migration (De Valk at all. 2022).

Finally, the recent migrant flows provoked by the war in Ukraine are taking place in addition to the previously affected countries with refugees and migrants' inflows and internally displaced people. It should not be underestimated that this current situation can grow into a long-lasting challenge, so joint action is necessary today rather than tomorrow.

Turkey and North Macedonia have a profound experience how this issue can impede all spheres of society. We can work together, or, in other words, we are obliged to act.

The Russia-Ukraine War of the New Emerging and Disruptive Technologies

It has been more than a year since the illegal invasion of Ukraine began. The consequences are devastating in all aspects and for all of us. The Russia-Ukraine war is the most technologically advanced war that humanity has ever seen thus far. The war brought a new impact of use of technology and build-up of military and non-military instruments of power.

The digital technology plays an important, if not decisive, role in the Ukraine-Russia conflict. Despite all conventionality on the one hand, the best categorization of this war, on the other, is the "first cyber world war" in the twenty-first century, because the variety of technologies that have been used marked this conflict as the most technologically advanced war that humanity has ever seen.

Though much of the battle has taken place on the battlefield itself, there has also been a war of technologies, from hybrid warfare, cyber attacks and disinformation, satellites, communications, drones, electronic warfare, social media, artillery and missile systems, virtual reality, and to the economic impact on the global tech scene. The impact of the use of emerging and disruptive technologies on the ground has been devastating.

Even before it started, having in mind the importance of the emerging and disruptive technologies, NATO has launched a ground-breaking initiative to sharpen the Alliance's technological edge, also known as Defence Innovation Accelerator for the North Atlantic - DIANA. However, the delivery of technology outcomes at the battlefield justified DIANA to further concentrate on the development of deep technologies, especially those emerging and disruptive technologies that NATO has identified as priorities. They include, inter alia, and focus on: artificial intelligence, big-data processing, quantum-enabled technologies, autonomy, biotechnology, novel materials and space (DIANA 2023).

The war in Ukraine confirm the need for promotion, innovation and increased investments in emerging and disruptive technologies.

According to the Strategic Concept 2022, emerging and disruptive technologies bring both opportunities and risks. They alter the character of the conflict, acquiring greater strategic importance and becoming key arenas of global competition.

It is by far confirmed by the results at the battlefield.

Technological primacy increasingly influences the success, and thus, the development of Emerging and Disruptive technologies needs a coherent approach by NATO and the EU.

Regarding the use of the EDTs in the war in Ukraine, if we carefully analyse the beginning of the war, we can see that Moscow fired its first shots with cyber-attacks with a Trojan horse wiper malware, named "Fox Blade". The day before the ground invasion, the cyberweapons became a prelude to an all-out war. Computer systems in different Ukrainian ministries, government organisations, and banks were the targets of distributed denial of service (DDoS) attacks (McGee-Abe 2023). The aim of this cyberattack was to paralyse Ukraine's command and control centres. Cyberattacks and disinformation strategies play an integral part in the conflict. Besides states and their affiliated cyber proxies, various cyber groups and cyber gangs are taking sides, as well in ransomware opportunity, increasing the risk of escalation.

These cyberattacks are perpetual even today and many of the countries are faced with it. For example, in North Macedonia we have had more than five months' constant cyber-attacks on state institutions, including the last one on the Health Care Insurance Fund. These cyber activities were complementary with hybrid warfare which includes fake bombs announcements in the schools, various ministries and even the presidential residence. We are witnessing every day disinformation campaigns and fake news through the social media platforms. We are all familiar with the way this news and disinformation has been spread through social media platforms creating a so-called “battle of narratives”. The war in Ukraine has become the most internet-accessible war in history with live updates and videos published through various social media platforms.

It should be recognized that despite all those constraints that war is bringing along, Ukraine has been able to use social media locations to be able to target specific groups of Russian soldiers. In addition, we should not underestimate the importance of the outer space domain that has proven its growing importance.

Outer space is becoming a more important domain of warfare every day. More than 5,000 Starlink satellites (Tsereteli 2022) were initially sent in the days after Russia’s full-scale invasion. Keeping the Internet running has been critical to help Ukraine’s citizens stay connected, but also to aide Ukraine’s defensive coordination. This is really the first major war in which commercially available satellite imagery may play a significant role in providing open-source information about troop movements, military build-ups in neighboring countries, flows of refugees, and more. To date, around 25,000 Starlink terminals (McGee-Abe 2023) have been deployed to assist Ukraine’s defence and connectivity efforts. We cannot forget the significant use of electronic warfare systems, which are used to disrupt communications, radar systems, and other electronics. These systems are used to jam communications systems on the both sides, thus the question remains how to be more efficient than the adversary (McGee-Abe 2023).

We should not forget also that as part of its self-perception as a great power in competition with the US and NATO, Russia has strived for more than a decade to demonstrate its ability to catch up and surpass its rivals in military technology. Drones and AI have been an important part of the political and military leadership’s narrative. They have not only been associated with strategic advantages, but also with the symbols of a modern military. To prove that its army is ready for 21st century combat, Russia has engaged in performative demonstrations via, among others, military parades, strategic exercises, and propaganda surrounding Moscow’s campaigns and operations.

We saw the results of this Putin’s politics on the battlefield because the war has featured more drone technology than any previously with both sides using unmanned aerial vehicles (UAVs) for reconnaissance and surveillance (Tsereteli 2022). The Ukrainian military has also used drones to target enemy positions with precision-guided munitions. The most used UAVs are simple, commercial drones, with integrated high-resolution cameras that are paired with smartphones. Soldiers have used them for intelligence, surveillance, and reconnaissance, which puts them one step ahead of the enemy. The Iranian, Chinese, Turkish drones carry laser-guided bombs and target vehicles, troops and military stations. As the use of drones has become more prevalent in the conflict, both sides have also developed counter-drone systems to detect and neutralize enemy UAVs. The Ukrainian military has reportedly used anti-drone systems such as the Turkish-made KARGU drone, which can autonomously track and attack targets (McGee-Abe 2023).

As early lessons identified and learned, we can speak about using virtual reality training systems to simulate combat scenarios and train soldiers in tactics and procedures. This type of training allows soldiers to practice in a safe and controlled environment before deploying to the front lines.

Although not always advanced technology supported the artillery, missile systems play an important role in this war. Putin's regime uses various types of artillery and missile systems, including rocket launchers, howitzers, and ballistic missiles, to shell Ukrainian-held territory and targets. By October 2022, more than 4,000 base stations, 60,000km of fiber-optic lines, and 18 broadcasting antennas had been seized, damaged, or destroyed, according to Ukraine's Special Communications Service (McGee-Abe 2023). However, the broadening of the perspectives of implementation of high-tech artillery systems in the future should not surprise likeminded militaries.

Conclusion

For more than a year, the world has been facing the consequences of Russia's aggression against Ukraine. The implications of the war are felt in every pore of human existence. The initial shock of energy and food shortages was followed by a drastic rise in prices and inflation. Now, the world economy is on its way to recover and strengthen its resilience against energy and other dependence on the East. A major challenge for Europe in the years to come is to implement the lessons learned from the war in Ukraine. The goal of the implementation of the lessons learned is to make Europe more resilient to future challenges, threats and risks to its security. The first lesson learned is the diversification of the energy supply and other materials. The war accelerated this process of reducing the energy dependence of European countries, primarily on Russian gas and oil. The process itself was helped by the United States, but with certain challenges related primarily to higher energy prices. By diversifying itself, Europe has become more resilient to Russian influence and blackmail.

The next element is the strengthening of multilateralism followed by the redistribution of power and the geostrategic competition between the West led by the US, NATO and the EU on the one hand and Russia, China and the BRICS on the other. The accession of Finland and Sweden to NATO is a positive signal for the expansion of the zone of free democracies, peace and security in Europe. However, the war in Ukraine has only one acceptable option for the democratic West, and that is the Ukrainian people must win the war against the Putin regime. It will be a success for NATO and a strong indicator of the strengthening of the effective multilateralism promoted by the EU. On the other hand, if the war goes in an undesired direction for Putin, Moscow may try to "freeze the conflict" and thus hold Europe's security "hostage" for a longer period. Such an option of a "frozen conflict" on European soil will not benefit anyone and will undermine the established European security architecture.

The war spurred a wave of migration of the Ukrainian people to the EU members. In this domain, the EU reacted quickly and activated its mechanisms and accepted migrants and refugees from Ukraine. This quick response of the EU is primarily the result of the need for labor in the European economy. In that context, most EU countries have taken measures for accelerated integration of refugees and migrants from Ukraine into national economies. Such an influx of new labor force had a positive effect on the economic growth of some of the EU members. It is very likely that a large part, especially those from the young category, will remain permanently in the countries where they are taken care of. This trend also depends on the post-conflict reconstruction of Ukraine, which will not be so fast and will take decades. The destruction on the ground and of the critical infrastructure is on a large scale.

The impact of the use of emerging and disruptive technologies on the ground has been devastating. Namely, the development of events on the ground and the use of different modern military platforms shows that it is a war in which the most advanced technologies are used. We are talking about military technologies that rely on artificial intelligence, satellite communications, drones, electronic warfare, artillery and missile systems, virtual reality, cyber-attacks followed by hybrid warfare tactics, "war of narratives" and disinformation spread through social and mass media.

The use of technology as an enabler of military and nonmilitary instrument of power by far is challenging all countries to consider a technological upgrade of warfare in the years to come. Both NATO and the EU have to keep up with research and development of the new emerging and disruptive technologies in all areas. NATO has already established DIANA with the aim to speed up the development of deep technologies, especially the emerging and disruptive technologies that NATO has identified as priorities (artificial intelligence, big-data processing, quantum-enabled technologies, autonomy, biotechnology, novel materials and space).

REFERENCES:

Botelho, Vasco. and Hannah Hägele (2023). Integrating Ukrainian refugees into the euro area labor market. 1 March 2023. https://www.ecb.europa.eu/press/blog/date/2023/html/ecb.blog.230301~3bb24371c8.en.html#:~:text=According%20to%20the%20United%20Nations,many%20cases%2C%20quitting%20their%20jobs.

BOFIT - The Bank of Finland Institute for Emerging Economies (2022) As the world's largest wheat exporter, Russia plays a major role in food security of Africa and the Middle East, 8 Jul 2022. https://www.bofit.fi/en/monitoring/weekly/2022/vw202227_v5/

CReAM – Center for Research &Analysis Migration (2023). Current migration flows from Ukraine. Last updated 15 February 2023. https://cream-migration.org/ukraine-detail.htm?article=3573

De Valk, Helga A. G. at all. (2022). "Introduction to Migration Studies", How to Predict Future Migration: Different Methods Explained and Compared. Chapter 28 pp. 463-482. https://link.springer.com/chapter/10.1007/978-3-030-92377-8_28.

DIANA (2023). Defence Innovation Accelerator for the North Atlantic. https://www.diana.nato.int/about-diana.html

Duszczyk, Maciej. And Pawel Kaczmarczyk (2022). The War in Ukraine and Migration to Poland: Outlook and Challenges. Intereconomics, Review of European Economic Policy, Volume 57, 2022 · Number 3 · JEL: F22, O15, R23. https://www.intereconomics.eu/contents/year/2022/number/3/article/the-war-in-ukraine-and-migration-to-poland-outlook-and-challenges.html#:~:text=The%20war%20initiated%20by%20Russia,over%2095%25%20were%20Ukrainian%20citizens.

Freedman, George. (2010), George Friedman's "The Next 100 Years; A Forecast for the 21st Century" , European Affairs, https://www.europeaninstitute.org/index.php/93-european-affairs/february--march-2010/962-george-friedmans-the-next-100-years-a-forecast-for-the-21st-century

Garver, Rob (2023) Ukraine Begins Plans for Post-War Reconstruction. February 14, 2023. https://www.voanews.com/a/ukraine-begins-plans-for-post-war-reconstruction/6963528.html

Jenkins, Michael Brian (2023) Consequences of the War in Ukraine: The Economic Fallout, March 7, 2023, https://www.rand.org/blog/2023/03/consequences-of-the-war-in-ukraine-the-economic-fallout.html

Jenkins, Michael Brian, (2023a), Consequences of the War in Ukraine: The End and Beyond, March 8, 2023, https://www.rand.org/blog/2023/03/consequences-of-the-war-in-ukraine-the-end-and-beyond.html

KPMG, (2022). Russia and Ukraine conflict: Economic implications, 7 March 2022, https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2022/03/russia-ukraine-conflict-yael-selfin-piece.pdf

Lagarde, Christine (2022) Monetary policy in a high inflation environment: commitment and clarity. 4 November 2022, https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp221104_1~8be9a4f4c1.en.html

OHCHR - Office Of The High Commissioner for Human Rights (2023) Ukraine: civilian casualty update 13 March 2023, March 13, 2023. https://www.ohchr.org/en/news/2023/03/ukraine-civilian-casualty-update-13-march-2023#:~:text=This%20included%3A,2%2C610%20killed%20and%205%2C958%20injured).

McGee-Abe, Jason. (2023). One year on: 10 technologies used in the war in Ukraine. Tech Informed, February 24, 2023. https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine/

Minakov, Mykhailo., Hanna Shelest, Tetyana Malyarenko & 2 more, (2023). Assessing the Outcomes of Russia's War on Ukraine, January 23, 2023, https://www.wilsoncenter.org/blog-post/assessing-outcomes-russias-war-ukraine

NBC NEWS (2022). More than 10,000 Ukrainian troops killed in war, official says. Dec. 2, 2022. https://www.nbcnews.com/news/world/10000-ukrainian-troops-killed-war-russia-invasion-rcna59780

Radio Free Europe/ Radio Liberty (2022). Russian Energy Export Revenue to Rise By 'Almost $100 Billion' This Year, August 17, 2022, https://www.rferl.org/a/russia-energy-export-revenue-rise/31993030.html

The World Bank (2022) Ukraine Recovery and Reconstruction Needs Estimated $349 Billion. Press Release 2023/ECA/11, September 9, 2022. https://www.worldbank.org/en/news/press-release/2022/09/09/ukraine-recovery-and-reconstruction-needs-estimated-349-billion

The World Bank (2023), Food Security Update, March 23, 2023. https://thedocs.worldbank.org/en/doc/40ebbf38f5a6b68bfc11e5273e1405d4-0090012022/related/Food-Security-Update-LXXXI-March-23-2023.pdf

Tsereteli, Aleksandre. (2022). Use of Technologies in the Russia-Ukraine War. August 2, 2022. Friedrich Neumann Foundation https://www.freiheit.org/ukraine-and-belarus/use-technologies-russia-ukraine-war

Trismpioti, Asimina. (2023) The Secretary General's Annual Report 2022, March 21, 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/sgar22-en.pdf#page=51&zoom=100,0,0

UNHCR (2023). Ukraine Refugee Situation. UNHCR Operational Data Portal, Accessed April 4, 2023. https://data.unhcr.org/en/situations/ukraine

Scientific article
UDK 316.776.23:355.48(470+571:477)"2022/2023"
UDK 316.774:32.019.51:[355.48(470+571:477)"2022/2023"

FAKE NEWS AS PART OF THE INFORMATION OPERATIONS DURING RUSSIA - UKRAINE WAR

Igor GELEV[1]
Biljana POPOVSKA[2]

Abstract: *The armed conflict between Russia and Ukraine has caused tectonic upheavals at the international political scene. Hence, the emerging fear of a new World War has determined the role of the international community in dealing with the consequences of such large military conflicts. Regrettably, such armed conflicts have resulted in catastrophic consequences for the lives of the civilian population, a large number of human losses, almost 10 million refugees and displaced persons, as well as a humanitarian disaster of epic proportions.*

Concurrently, the world is facing the possibility of an ecological disaster (nuclear disaster) whose consequences are difficult to predict too. In addition, energy crisis has slowed down the technical-technological development of the industrialized countries, which has resulted in an increase of the prices of almost all commodities. Consequently, poverty in all countries has increased, especially in the countries dependent on Russian energy. Finally, the instability of the trading markets also discourages investors as the basic financial source for consumer societies thus further complicating the overall economic situation.

To this end, hybrid research has been carried out to determine the fake news during this conflict and their impact on the Macedonian population.

Fake news is created to achieve political, economic or military supremacy over a particular state, political or economic subject. Thus, through social media, true, semi-true and false information is created and disseminated for a particular auditorium to influence their emotions, motives, morals and desires. At the same time to influence the behavior of state and non-state actors.

Key words: *Fake news, Soft power, Disinformation.*

Introduction

Clausewitz has defined war as an extended arm of politics, i.e., continuation of politics by other means. However, this armed conflict is multilateral. To be more precise, the armed conflict has been multiplied by an economic war (economic sanctions against Russia from the Western countries. The Russian side has imposed energy payments in Russian currency on enemy countries). In addition, there is a diplomatic war (the G20 Summit, initiation of the Hague Tribunal for war crimes, condemnation or support for one of the parties to the conflict,

[1] Dr. Igor Gelev is a Colonel in the Armed Forces of the Republic of North Macedonia. The research and views expressed in this paper are solely of the authors and are not related to the institution they come from.

[2] Mrs. Biljana Popovska is an adviser in the Ministry of Defense. She is a PhD student at the University of Bucharest, Romania

condemnation of Russian aggression as a condition for admission in the EU pertinent to the candidates' countries). Also, redefinition of the UN (an initiative to exclude Russia from the Security Council) and, certainly an energy war (which the Arab energy exporting countries also joined). In parallel, various non-state actors also have had an impact. Such is the case of Elon Musk who provided satellite internet for the Ukrainians, annulling the media cut off due to the armed conflict, and the hacker group Anonymous, with its cyber-attacks on Russian infrastructure. The overall situation will most likely culminate in a new bloc division and a complete redesign of the international political scene.

What each of the aforementioned components has in common is the media support in justifying the individual goals. In the part which tackles media war, this paper will discuss INFO operations as an indispensable part of the strategic concepts for warfare of the armies in the world, although nowadays they are modus operandi for another type of warfare of (non)state actors, i.e., for political, economic and ideological warfare

Info war between Russia and Ukraine

Social media as an alternative to other mass media became dominant as a result of political, academic and business relations with the outside (more distant) world, certainly referring to Europe, America and Asia. Since 2018, approximately 900 000 people have gone online for the first time on a daily basis. Currently, there are more than 5 billion active internet users around the globe. After the pandemic hit the world, the number of internet users has increased tremendously, and most of the education, work, and other communications are done online.[3] Obviously, the role of social media in creating opinion on the international and domestic political scene is significant. Numerous political and military analysts have devoted time to exposing the power of the Internet as a medium that has a major impact in shaping public opinion.

However, in conditions of hard power (conventional armed conflict) there is no time to create public opinion with half-truths. Instead, fake news is mostly used. Namely, the events are dynamic and most of the time each of the opposing sides uses fake news to demonize the other side or justify their violence. What is characteristic during this

[3]

1. 5.07 billion people around the world are on the internet as of 2023.
2. 63.5% of the world population has access to the internet.
3. Thanks to accessibility to mobile phones, more than 170 million internet users appeared in the time span of one year.
4. Internet users are reported to increase at an annual rate of 3.5 percent.
5. Less than 3 billion people are not connected to the internet in Southern and Eastern Asia and Africa.
6. 92.1% of internet users use mobile phones to browse the internet.
7. 60% of the world's web traffic is made by mobile phone users.
8. More than two-thirds of global internet users use laptops and desktops for their online activities.
9. As of January 2023, the global reach of social media has grown to 4.74 billion people.
10. Between October 2021 and 2022, 190 million internet users joined social media.

Source: Cisco, eMarketer, Statista, broadband search.

armed conflict, is that one of the parties (Russia), has used half-truths and fake news even in the time before the conflict started. Hence, it influenced part of the audience (it was an audience that already had a side-taking role to one of the parties in the conflict). The rest of the audience not fully familiar with the dispute as the cause of the armed conflict was generally familiarized with the source of the armed conflict after the war in Ukraine began. In that way, this audience (which represents the largest percentage of the total audience) was influenced by the news that reported on the situation on the ground after the armed conflict began.

Looking back, at the beginning of the 2014 conflict, the Russian military adopted a new doctrine explicitly stating that information superiority is essential to achieving victory on the physical battleground in the modern war. Therefore, the Ukrainian case offers lessons potentially applicable to other NATO member states. For instance, in many cases Russia actively accuses the Baltic States on the same grounds as it accuses Ukraine as to deliberately discredit these countries in the international arena (e.g. accusations of rehabilitation of Nazism). To be more specific, Russia often adopts defensive narratives, which justify its positions in the mythologized opposition between the East and the West. The Ukrainian authorities, as well as the interested international organizations are considered to be puppets of the West under the guidance of the United States and NATO. The concept of Russian World is used as an ideological tool by Russian political elites as to unite all Russian speaking people worldwide and to create a powerful and global Russian speaking cultural, ideological, historical, social, political and informational space as an alternative to the Soviet Union. This concept of the Russian World is closely related to the compatriots' policy of the Russian Federation—Russia declared that its duty is to protect Russian-speaking people not only in Russia, but abroad too. The representation of these target groups in the media was scrutinized against the following labels and phenomena:

- Parallels with the Third Reich—fascists, Nazis, neo-Nazis, Banderivtsi etc.;
- Humiliation and belittlement of Ukrainian soldiers by, for example, calling them criminals, rapists, drug addicts, and cowards, or by claiming that there is an abundance of violence, chaos, etc., within the Ukrainian armed forces;
- Execution squads, punitive units (karateli);
- Genocide, fratricide, terrorists;
- Kyiv junta and its followers;
- Russophobia—discrimination, nationalism, xenophobia;
- Ukrainians as 'false Russians', little brothers, Ukraine as a failed state, the West as fascist;
- Ukrainians as puppets of the West;
- Western provocations against Russia in Ukraine (Dr. Vladimir Sazonov, 2015).

Tools of info warfare

The general doctrine emphasized by Russian media is the protection of the Russian-speaking population, denazification of Nazi (non)political movements, consolidation and protection of Orthodoxy (Russia sees Belarus and the Baltic States as part of the Russian World - Pax Russica. This is another reason why Russia perceives the Baltic States as geopolitical puppets of the West, civilization that 'dreams' of annihilating the so-called unique Russian Orthodox world). In addition, for the case of Crimea, Russia abandoned its conservative position on self-determination, presented to the International Court of Justice in 2009 in connection with Kosovo's unilateral declaration of sovereignty and adopted the liberal position by emphasizing that the Unites States had put forward the position in the same proceedings.

Propaganda war from 2014 still plays a growing role in the confrontation between Russia, Ukraine, and Western countries. However, the criteria and definitions of the success in this war have been in constant development during the last period of the confrontation. The central activities of Russia focus on demonization and deterrence of the adversary, legitimization of one's own activities to the general audience, mobilization of population and promotion of political elites. In the light of public opinion polls on the support for their respective governments and opposition to their adversaries, all three parties have mostly reached their objectives. Nevertheless, the question is whether this is being considered as evidence of tactical success and a sustainable strategy in the longer run.

In summary, media news was available to the world public. It reported that Russia is the aggressor in the war with Ukraine (according to international law), highlighting Putin's crazy desire to return the USSR or the territories from the time of Tsarist Russia. Domestic corruption in Russia, totalitarianism, Pan-Slavic movement, clash of civilizations, coordinated and orchestrated activity of China and Russia are also cited as the causes of the armed conflict, and the fact that the armed conflict in Ukraine is a threat to Western and civilizational values has been widely reported. But unlike the conflict in 2014, Russia chose silence in the armed conflict with Ukraine as a new methodology of INFO warfare. Specifically, it seemed to create the conditions for the Russian media (electronic, television, and audio) to be inaccessible to the world public through their exclusion from the West, which increased the control of media registered in countries outside the United States. At the same time, control of VPN services and IP addresses increased. Moreover, the criteria of marketing companies, which are a source of income for those who produce news about the armed conflict, were tightened. Thus, Russia tactfully made points through media intolerance on the world media stage. Namely, the only news about the war in Ukraine that was available to the world public was the news from the Western media (especially from the world mainstream, which had previously undermined its credibility among the world public through various propaganda activities). At the same time, frustration appeared among the public due to the impossibility of hearing the other side. Particularly negative impact was the exclusion of everything that had a Russian sign – sports events, cultural events, educational events and the like.

Effects of political news

Generally, the effects of political news have a great impact on the population affected by the relapses of the war (military threats, economic consequences, fear of bilateral disputes with some of the neighbors). The purpose of such news is three- folded. The first one is commercial use and pure earnings from an audience that perceives itself as part of the population victim of the aggressor. The second moment (also a problem) is the censorship of certain media (we are talking about the mega-popular media) which have created an opinion about society and the world for decades and impose a media culture, declare themselves as a tool of the democratic society, although they use undemocratic means. And thirdly, there is (un)clear connection between powerful media and multinational corporations with their own supranational interests. However, as the available data display there is a common goal underneath. It is continuation of the war in Ukraine.

Electronic media as a tool for spreading fake news

Fake news is created in order to achieve political, economic or military supremacy over a certain state, political or economic subject. Thus, through social media true, half-true and false information is created and disseminated for a specific audience in order to influence their emotions, motives, morals and desires, and at the same time to influence the behavior of state and non-state actors. To conduct the research for this paper, statistics on the use of electronic media, i.e., social networks were observed.

Social Media Statistics

When it comes to internet usage, most of it relates to social media sites. Most internet users start their day by logging into their social media accounts. It is reported that the most used applications online are the social media apps. Here are a few available stats related to social media usage:

1. 59% of the world's population uses social media. Out of 5 billion internet users, 4.7 billion are on the social media;
2. Facebook was the first social media platform to surpass more than one billion accounts registration. Today there are approximately more than 2.89 billion active users on Facebook;
3. YouTube reported to have 2.5 billion active users, while Whatsapp has 2 billion active users;
4. Here is the data representing the active users on different social media platforms:

Social Media Platform	Users Worldwide
Facebook	2.9 billion
YouTube	2.5 billion
What Sapp	2 billion
Instagram	1.478 billion
Weixin/ We Chat	1.26 billion
TikTok	1 billion
Facebook Messenger	988 million
Douyin	600 million
QQ	574 million

5. In the year 2021, social media users worldwide were reported to be 4.480 billion;
6. Facebook was recorded to be the third most visited website in the world;
7. The most downloaded app in the year 2021 was Tiktok;
8. Facebook is the primary social media app used by 68% of Americans, while Instagram is the second most used app with 35% of the users, and Pinterest is third with 29% of American users;
9. Only 35% of Facebook users are below the age of 35;
10. 88% of the traffic on Facebook was reported from mobile devices;
11. 80% of Instagram users are located outside of the United States;
12. 38% of Instagram users will check their applications more than once per day.

Source: Cisco, Statista.

Video statistics

1. 82% of internet traffic in the year 2021 came from video streaming;
2. There are more than 1.8 billion unique monthly visitors on YouTube;
3. Here is the data related to the most visited video sources on the web:

Platform	Monthly Visitors
YouTube	1.8 billion
Netflix	150 million
Vimeo	130 million
Yahoo! Screen	125 million
Dail motion	100 million
Hulu	75 million

4. 45% of the people reported watching online video content for an hour or more;
5. It was reported that 50% of users between the age of 18 and 34 would drop their current task and watch a video on a channel they just subscribed to;

6. 40% of the millennials have trust issues or high-quality content on YouTube;
7. 50% of the people watch videos of the products and their demos before buying them;
8. If a person watches more than 6 minutes of a video then it is likely that they will watch the whole video;
9. 90% of the video view on Twitter are recorded through mobile;
10. There is a 95% increase in the expenditure of video-based advertising.

Source: eMarketer, Statista

Search Statistics

Search is the main task carried out with the help of the internet. It is used to search all the crucial data worldwide. Most internet users mostly use their data to browse by using search engines.

1. Google is responsible for 92.01% of the search engine market share;
2. Even for the mobile search engine, market share is ruled by Google with 95.23% of users worldwide;
3. Google processes 3.5 billion searches on daily bases. It equals up to 1.2 trillion searches each year and sums up to 40,000 per second;
4. Google owns 83.84% of the global share in the search market;
5. 61.7% share of Google sites is owned by the US market;
6. 2.55% of the worldwide market share of desktops belongs to Yahoo!
7. 26.2% of the US search market share belongs to Microsoft Sites;
8. Baidu owns 76% of the search market share in China;
9. 42% of internet users conduct voice searches globally.
10. 93% of the mobile search market share in the US belong to Google.
11. 23% of Bing's organic traffic is from mobile searches.
12. The mobile share of Google's organic search traffic is 61%.

Source: Statista, Cisco.

Media news about the armed conflict in Ukraine and their impact on the Macedonian population

Fake news is daily occurrence on the Internet and have had a great influence in shaping public opinion.4 According to research conducted by the authors of this text creation of fake news and its dissemination through the social media differs from the creation of fake news during the US presidential elections in 2016. Then, there was a possibility of unlimited creation of FB avatars and unlimited sharing of Fun Pages and Groups with thematic content. Later for the 2020 US presidential election, social networks such as Facebook, Twitter and Reddit improved their algorithms to find fake

[4] Psychological operations Techniques and Procedures, FM 33-1-1, Washington, DC, 5 May 1994 (pg. 9-9)

news (text, image and video) and promptly removed content that lacked informational credibility (news source, author-journalists, research or scientific institute behind the information).

In addition, companies dealing with online commercial advertising have tightened the criteria for awarding ads, especially for owners of newly created websites, as well as pages that deal with politics or so-called sensational news in which the key actors are politicians and celebrities involved in the political campaign.

It was evident that during this presidential campaign, fake news was replaced by sensational news that managed to avoid the fake news algorithm (they were not properly supported by credible sources). At the same time, such news were shared by both political camps and caused great interest among the politically undecided population.

During the Russian-Ukrainian war, a content analysis related to the course of the war was made, and different results were obtained depending on the type of content and the time (the period of the conflict) of the war.

For this purpose, we, the authors of this paper, carried out research in three Facebook groups with over 50,000 members where news about the Russian-Ukrainian war is shared firstly covering the period from 2 July to 3 August. Then, the period from 5 September to 1 October, and the third one is the period from 1 December to 31 December. In doing so, we compared the news that was shared according to these three categories. The first category is the term Russian aggression. The second category is Ukraine as a NATO member, and the third category is the annexation of Ukrainian territory (contrary to the UN Charter).

A Facebook group is a unit of content analysis. The results are mutually analyzed, semantically linked and compared by using the Semantic Text Analysis Software.

Chart 1. Russian Aggression

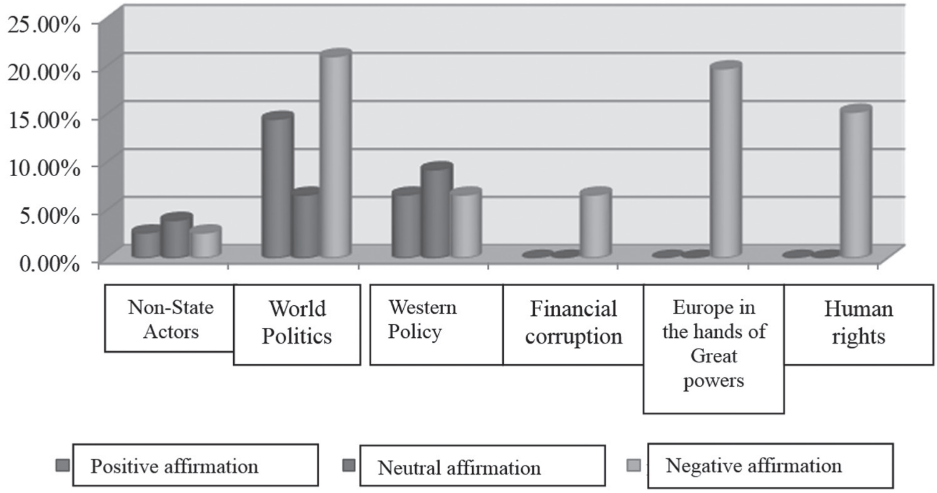


Table 1. Russian Aggression

Subcategory	**Total texts**	+	**0**	**-**
Total	**76 (100%)**	**18 (23.68%)**	**15 (19.73%)**	**43 (56.57%)**
Non-state actors	7 (9.21%)	2 (2.63%)	3 (3.94%)	2 (2.63%)
World politics	32 (42.1%)	11 (14.47%)	5 (6.57%)	16 (21.%)
Western policy	17 (22.36%)	5 (6.58%)	7 (9.21%)	5 (6.58%)
Financial corruption	5 (6.58%)	0	0	5 (6.58%)
Europe in the hands of the Great Powers	15 (19.73%)	0	0	15(19.73%)
Human rights	7 (15.21%)	0	0	7 (15.21%)

The data are obtained by the use of the analytical software *Tropes* with semantic analysis of certain words in the texts that gravitate around the phrase Creating a world government. Additionally, statistical analysis was performed with the Semantic Text Analysis Software.

The analysis was conducted on a total of 76 texts and the whole category is divided into 6 subcategories. They were analyzed whether they had a positive, negative or neutral affirmation and the percentages are given from the total number of analyzed texts and not only from the given subcategory. So, when we analyze the term *non-state actors* in the content of the published texts on this topic (out of a total of 7 texts, 2 texts or 2.63% have a positive affirmation, 3 texts or 3.94% have a neutral affirmation and 2 texts or 2, 63% have a negative affirmation). Then, in the *World Politics* subcategory (as a result of the political antagonism in the World, divided into East and West), most of the texts have a negative affirmation (16 texts or 21% of the total number of published texts in the Russian aggression category). It is striking that newspapers and television exploit the term world war much less than the social media (we take social media with freedom of speech in the form of emoticons, comments and shares as a benchmark). A subcategory *Western Policy* follows, where in the content of the published texts on this topic (out of a total of 17 texts, 5 texts or 6.58% have a positive affirmation, 7 texts or 9.21% have a neutral affirmation and 5 texts or 6.58% have a negative affirmation). The subcategory *Financial Corruption* (refers to financial corruption in Russian society, Ukrainian society, but also among certain Western politicians has an absolutely negative affirmation (all texts have a negative affirmation), which testifies to the fact that the public does not support it, that is, it represents a negative variable in the war. The subcategory *Europe in the hands of the great powers* also has a negative affirmation (all texts from this subcategory have a negative affirmation), which testifies that the audience in Macedonia supports an independent policy of the European states, especially in the Russian-Ukrainian conflict. The subcategory *Human Rights* in the content of the published texts on this topic (out of a total of 7 texts all have a negative affirmation) has a negative affirmation, i.e., the audience believes that human rights have been violated as a result of brutal crimes against the civilian population in Ukraine, but also against the pro-Russian civilian population in the crisis regions.

Chart 2. Ukraine as a NATO member

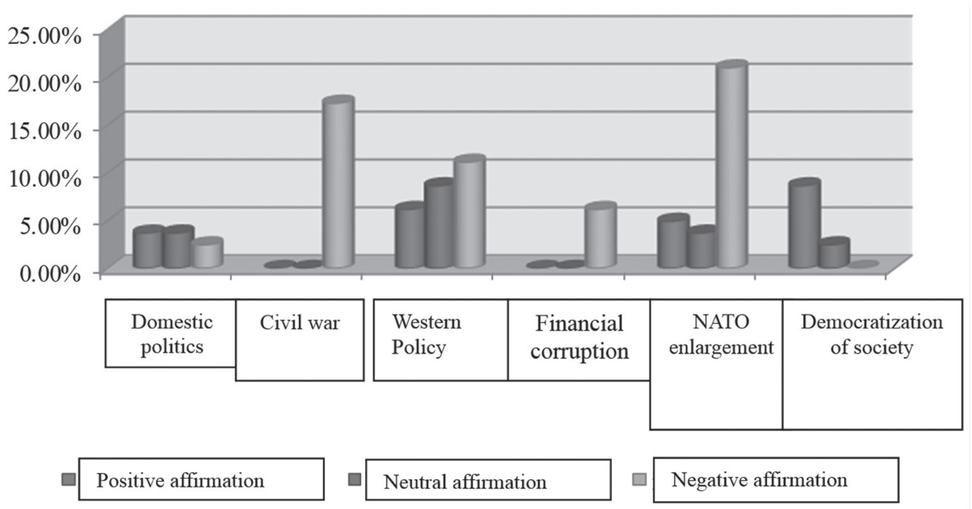


Table 2. Ukraine as a NATO member

Subcategory	Total texts	+	0	-
Total	**81(100%)**	**19 (23.45%)**	**15 (18.51%)**	**47 (58%)**
Domestic politics	8 (9.87%)	3 (3.7%)	3 (3.7%)	2 (2.47%)
Civil war	14 (17.28%)	0	0	14 (17.28,%)
Western policy	21 (25.92%)	5 (6.17%)	7 (8.64%)	9 (11.11%)
Financial corruption	5 (6, 17%)	0	0	5 (6.17%)
NATO enlargement	24 (29.62%)	4 (4.93%)	3 (3.7%)	17(20.98%)
Democratization of society	9 (11.11%)	7 (8.64%)	2 (2.47%)	0

The analysis was carried out on a total of 81 texts and the whole category is divided into 6 subcategories. They were analyzed whether they had a positive, negative or neutral affirmation and the percentages are given from the total number of analyzed texts and not only from the given subcategory. So, when we analyze the term *Domestic Policy* in the content of the published texts on this topic, out of a total of 8 texts, 3 texts or 3.7% have a positive affirmation, 3 texts or 3.7% have a neutral affirmation and 2 texts or 2 .47% have a negative affirmation. Then, in the subcategory *Civil War* (as a result of the political antagonism in Ukraine, divided between the population inclined towards Russia and the population inclined towards Ukraine), all texts have a negative affirmation (14 texts or 17.28% of the total number of published texts in the category Ukraine as NATO member). This means that everyone is in solidarity with the numerous civilian victims and suffering of the two peoples living on that territory. In the *Western Policy* subcategory in the content of the published texts on this topic, out of a total of 21 texts, 5 texts or 6.17% have a positive affirmation, 7 texts or 8.64% have a neutral affirmation and 9 texts or 11.11% have a negative affirmation. In general, it is due to the fact that most of them believe that the *Western Policy* influenced the instigation of the war in Ukraine. The subcategory *Financial Corruption* has an absolutely negative affirmation (all texts have a negative affirmation) which testifies to the fact that the public does not support it, that is, it represents a negative variable in the war. In the *NATO Enlargement/Expansion subcategory*, the largest number of texts have a negative affirmation. That is, the majority of the audience believes that the attempt for Ukraine to join NATO represents a trigger for the start of a Great War. This is also evident from the statistics, where out of a total number of 24 texts on this topic, as many as 17 texts (or 20.98% of the total number of texts from the whole category) are with a negative affirmation.

The subcategory *Democratization of societies* in the content of the published texts on this topic (out of a total of 9 texts, as many as 7 texts or 8.64% have a positive affirmation, and only 2 texts or 2.47% have a neutral affirmation. There are no texts with a negative affirmation that testifies to the support for democratization of societies as a western benefit in the evolution of societies.

Chart 3. Annexation of (part of) Ukraine

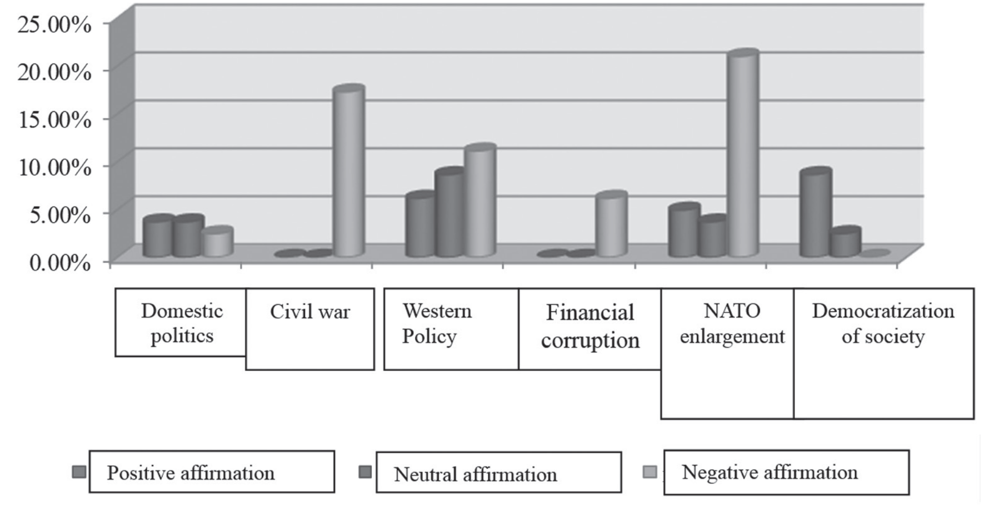
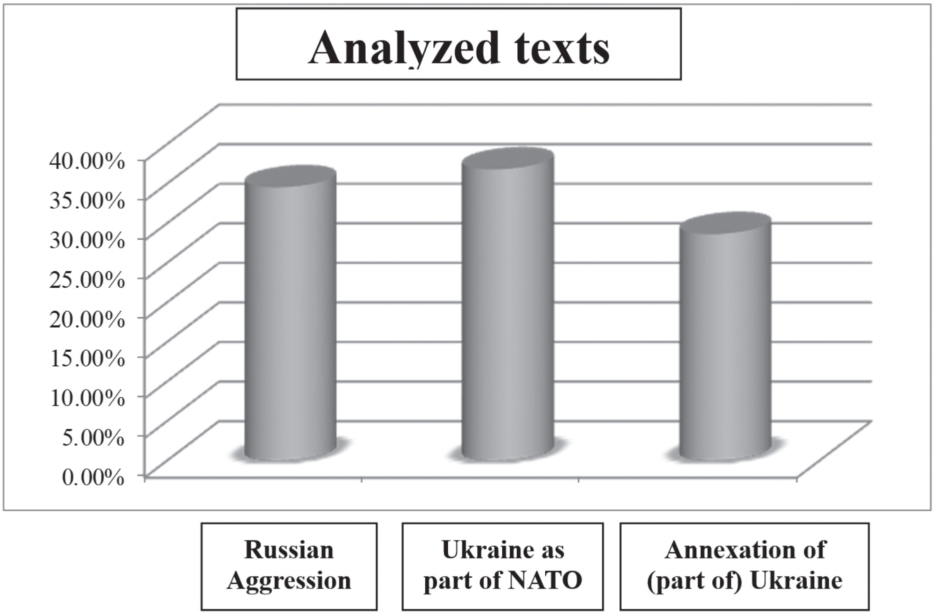


Table 3. Annexation of Ukraine

Subcategory	Total texts	+	0	-
Total	**63 (100%)**	**19 (30.15%)**	**6 (9.52%)**	**38 (60.31%)**
Russian history	18 (28.57%)	7 (11.11%)	3 (4.76%)	8 (12.69%)
World politics,	7 (11.11%)	3 (4.76%)	1 (1.58%)	3 (4.76,%)
UN- international law	5 (7.93%)	5 (6.58%)	0	0
Territorial secessionism	12 (19.04%)	4 (6.34%)	2 (3.17%)	6 (9.52%)
Kosovo as a case	15 (23.8%)	0	0	15(23.8%)
Human rights	6 (9.52%)	0	0	6 (9.52%)

The analysis was carried out on a total of 63 texts and the whole category is divided into 6 subcategories. They were analyzed whether they had a positive, negative or neutral affirmation and the percentages are given from the total number of analyzed texts and not only from the given subcategory. So, when we analyze the term *Russian History* in the content of the published texts on this topic (out of a total of 18 texts, 7 texts or 11.11% have a positive affirmation, 3 texts or 4.76% have a neutral affirmation and 8 texts or 12.69% have a negative affirmation). It is due to the negative experience of the Macedonians from the dispute with Bulgaria, when a country, referring to historical dogmas, makes territorial claims against another country. Then, the subcategory *World Politics* (as a result of the political antagonism in the World, divided into East and West) 3 texts have a positive and three have a negative affirmation, and 1 text has a neutral affirmation. The subcategory *UN - international law* follows, where in the content of the published texts on this topic, out of a total of 5 texts, all of them have a positive affirmation, that is, international law is supported. The subcategory *Territorial Secessionism* (refers to the secession of part of the territory of an independent and sovereign state contrary to the *Charter of the UN and International Law*), 6 texts or 9.52% of the total number of texts from the entire category have a negative affirmation, which testifies that the public does not support it, that is, secessionism represents a negative variable in the war). The subcategory *Kosovo as a case in point*, has 15 texts and all of them have a negative affirmation or 23.8% of the entire category, which also represents the highest negative variable (Macedonians have a fear of secessionism following the Kosovo scenario). The subcategory *Human Rights* in the content of the published texts on this topic (out of a total of 6 texts all have a negative affirmation) has a negative affirmation, that is, the audience believes that human rights are violated as a result of the violent annexation of a sovereign country.

Chart 4. Analyzed texts



Out of a total of 220 analyzed texts, 81 texts refer to the category *of Ukraine as a member of NATO*, which represents 36.82% of the total number of analyzed texts, 76 texts refer to *Russian Aggression* or 34.54%, and 63 texts to the *Annexation of Ukraine* or 28.63% of the total number of analyzed texts.

Conclusion

Social media create and design various political and socio-economic or security situations with the help of (non)state actors. Fake news play great role in creating public opinion and can imply a number of political and security conditions. On the other hand, social networks and groups have become virtual alliances of like-minded people (regardless of nationality, gender and other type of affiliation) who convey the message to those on the "other" side with a lot of energy.

According to the research done on the Russian-Ukrainian war, it is concluded that at the beginning of the special operation (as the Russian side called it), public opinion in Macedonia was absolutely on the side of Ukraine, if taking into account the similarities which Macedonia also faces, such as the appetites of some of its neighbors. Also, in the groups in which the war was reported, all the comments expressed solidarity with the civilian population suffering in the war. Especially the Ukrainian civilian population, considering that the war was fought on the territory of Ukraine. In the second period of the research, there was noticeable sharing of video contents in which there were explicit scenes of violence and murders carried out by both sides. As a result, and especially on the *Nazism* subcategory, the support for Ukraine has declined.

At the same time, there was a significant change in the content and information shared on social media. Namely, Fake news (in the form of text, image or video) was minimized, that is, it was deleted/cleared or had no reach and availability to the audience at all.

It indicates that social media, (especially Facebook), has made great strides in combating fake news and violent scenes and videos. But that caused a large part of internet users to switch to the Telegram social network.

It determined the role of people who were making money from fake news to switch to Telegram and through the creation of channels and groups to make commercial income. Namely, this social network is used mainly because of the (un)restrictions on the posting of content which, due to the imposed standards and criteria, cannot be posted on other social networks.

REFERENCES:

Archer Clive. *International Organizations*. 3 rd ed. London, 2001.

Ambrosius Lioyd E. *Woodrow Wilson and the American Diplomatic Tradition: The Treaty Fight in Perspective*. Cambridge University Press, 1990.

Drew Thompson. China soft power in Africa: from the "Beijing Consensus" to health diplomacy. s.n.2005

Elliot Harris, *The "Un-American" weapon: Psychological warfare* (New York: M.W. Lads Publishing, 1967).

Gagea Andreea. *Diplomacy in the Games of Power. Diplomacy of Power – Power of Diplomacy.* Bucharest Academy of Economic Studies. 2011.

Gallarotti, Giulio M., "Soft Power: What it is, Why it's Important, and the Conditions Under Which it Can Be Effectively Used" (2011). *Division II Faculty Publications.* Paper 57.

Glen Fisher. *Public Diplomacy and the Behavioral Sciences* (Bloomington, IN: Indiana University Press.1972).

Glen Fisher. *American communication in a global society.* Ablex Publishing Corporation, 1987.

Halliday F. "The Romance of Non-State Actors," In: D. Josselin and Wallace, Eds., *Non State Actors in World Politics*, Palgrave, London, 2000.

Ham van Peter. European Integration and the Postmodern Condition: *Governance, Democracy, Identity.* Routledge, Milton Park Oxon, 2001.

Hun Yun Seong. **"**Toward Public Relations Theory-Based Study of Public Diplomacy: Testing the Applicability of the Excellence Study," *Journal of Public Relations Research* 18, no. 4, (2006).

J. A. Scholte, "Globalisation and Collective Identities," In: J. Krause and N. Renwick, Eds., *Identities in Interna- tional Relations*, St. Martin's Press, New York, 1996.

James Dewar A. *"The Information Age and the Printing Press: Looking Backward to See Ahead*, RAND Paper No. 8014, 1998.

James P. Muldoon. Multilateral Diplomacy and the United Nations Today. Westview Press 2en. ed. 2005.

Joe Johnson, "How Does Public Diplomacy Measure Up?" *Foreign Service Journal* 83, no. 10, 2006.

Katzenstein Peter J. and Robert O. Keohane, “Anti-Americanisms,” *Policy Review* (October/November 2006),

Kennedy Paul, *The Rise and Fall of the Great Powers* (New York: Random House), 1987.

Kissinger Henry. *Diplomacy*. Simon & Schuster, 2011.

Mustonen J. *Case Study: Hard Power or Soft Power? Searching for China use of Soft Power in the pursuit of the economic cooperation framework agreement with Taiwan*, 2010.

Nye Joseph, *Soft Power: The Means to Success in World Politics*, 1st ed. (New York: Public Affairs, 2004).

Nye Joseph., *Bound to Lead: The Changing Nature of American Power* (New York: Basic Books, 1990); and J. Nye, *Soft Power: The Means to Success in World Politics* (New York: Perseus, 2004).

Po-chi Chen. *Cyber Public Diplomacy as China’s Smart Power Strategy in an Information Age: Case Study of Anti-Carrefour Incident in 2008*. InterCnyabetiro Pnuablli J Douiprlonmaal coy fa Cs Chhiin-naa’ sS Stmudarite Psower, 2012.

Shirky, Clay. “The Political Power of Social Media.” *Foreign Affairs,* January/February, 2011.

Vuving Alexander L. *How Soft Power works?* A American Political Science Association annual meeting, Toronto, September 3, 2009.

Zengotita de Thomas. *How The Media Shapes Your World And The Way You Live In It*. Bloomsbury, 2005.

Scientific article
UDK 355.48:341.311(497.15:4-672ЕУ)”1992/1995”
UDK 355.48:341.311(497.15:100-622НАТО)”1992/1995”
UDK 355.48:341.311(477:4-672ЕУ)”2022”
UDK 355.48:341.311(477:100-622НАТО)”2022”

COMPARATIVE ANALYSIS BETWEEN AGGRESSION ON BOSNIA AND HERZEGOVINA AND AGGRESSION ON UKRAINE IN TERMS OF NATO AND EU INTEGRATIONS

Emina MUŠIJA[1]

Abstract: *Aggression on Bosnia and Herzegovina started in 1992 and lasted until 1995, where Serbian and Croatian aggressors had an objective of dividing Bosnia and Herzegovina into geographical parts which would result in strengthening territorial capacities of the Republic of Croatia and the Republic of Serbia. Aggression on Ukraine started in 2022 when Russia launched a large-scale invasion by Russian president Putin's decision to authorize the so called special military operations in Ukraine. The similarities between these two wars are the invasion of a neighboring country with the aim of territorial annexation from a smaller country and the path of those smaller, invaded countries, towards NATO and the European Union. This paper will analyze the similarities between mentioned aggressions and how it affects the NATO and EU membership in detail. Additionally, the paper will elaborate the impact of the international community in these events.*

Key words: *Ukraine, Bosnia and Herzegovina, aggression, NATO, European Union.*

Introduction

On 24 February 2022, the world population was awakened with horrific news headlines: “The war has started”. On that day, the Russian army attacked Ukrainian borders with Vladimir Putin's announcement for “demilitarization and denazification of Ukraine”.

Similar news woke up citizens of Bosnia and Herzegovina in the spring of 1992 when Bosnian Serbs attacked Bosnia. What is common in both the Ukrainian and Bosnian war? Well, neighboring countries had an idea of creating bigger countries, in the case of Bosnia it was "Velika Srbija" and "Velika Hrvatska", while in case of Ukraine, it was the annexation of territories Luhansk, Donetsk, Zaporizhzhia and Kherson.

What was the first trauma trigger for Bosnian people was seeing images from Ukraine, devastated homes, buildings, bodies on the streets. Quite alike to the Bosnian soil in 1990s. Aggression on Ukraine created many triggers, not only for Bosnian people, but also for citizens of the entire Western Balkans, especially those that were part of the Socialistic Federative Republic of Yugoslavia.

The objective of this paper is to analyze the abovementioned similarities between the aggression on Bosnia and the aggression on Ukraine through comparison of the impact of the international community and the reasons for attacking neighboring countries. The focus during

[1] PhD Candidate at University of Ljubljana, Slovenia.

the research will be on analysis of reasons and consequences of the aggression. Finally, this paper will provide conclusion on what the aggression meant for the path of these two countries of interest towards NATO and the European Union.

Research conducted for the purposes of this paper was based on the qualitative means, by mostly using document analysis, comparison of cases that consists of the historical research and literature reviews. Document analysis will be conducted through primary and secondary sources, such as legal documents, original scientific papers, books and articles. Since the aggression on Ukraine is a relatively new event in the academia, internet sources will also be elaborated through analysis of media appearances. For the case of Bosnia and Herzegovina and bearing in mind the complexity of the war, meta-analysis will be used, in addition to the above mentioned research types. By using meta-analysis, previous research studies on the topic of war in Bosnia will be analyzed, elaborated and conclusions will be drawn upon the findings.

The significance of this research lies in the fact that this topic is important for the academic community and can serve as qualitative background for further research. In addition, it can be seen as comprehensive historical review of two countries' development in terms of aspirations for membership in two large international communities. Moreover, this paper will provide insight into the importance of drawing parallels in studies of war, peace resolutions and peace studies, specifically for countries that are politically, rather than geographically, connected.

Political history of Bosnia and Herzegovina

Bosnia and Herzegovina is a country whose history goes back to the 9th century. Throughout that history, Bosnia was many times part of the larger state, such as the Ottoman Empire, then Austrian-Hungarian Empire, then part of the Kingdom of Serbs, Croats and Slovenes and finally, part of the Socialistic Federative Republic of Yugoslavia. After the death of Yugoslavia's leader, Josip Broz Tito in the 1980s, events in all Yugoslav states started to increase the political dissatisfaction and aspirations towards independence (Pejanović, 2017). Mentioned political dissatisfaction was mostly notable in the countries' leaders whose nationalistic statements undermined the system that was already loosened and destabilized. First countries to seek for independence were Slovenia in 1990s and Croatia in 1991 by organizing multiparty elections (Ibrahimagić, 2009). Bosnia on the other side, also held elections in the 1990s that resulted in the creation of new parties whose aim was to represent three national communities – Bosniaks, Croats and Serbs (Pejanović, 2017). Not long after these elections in Bosnia, the leader of the Serbs formed the so called Serbian Autonomous Regions with the objective of declaring those areas as Serb-majority areas. The event of announcing the Serbian Autonomous Region was only the beginning of the separatist narrative and actions, continued by boycotting meetings of BiH's tripartite Presidency. The boycott led to the establishment of a Serbian National Assembly (Kulenović, 1998), as part of Bosnia's at the time, political system. Meanwhile, Croatia was fighting with the war itself which had already shaken the substantive vulnerability of Bosnia and Herzegovina.

Independence of Bosnia and Herzegovina was firstly recognized by the European Community at the time, on 6 April 1992. The United States of America was second to accept the independence only a day after (Ibrahimagić, 2009, Pejanović, 2017). One month later, Bosnia gets its membership status in the United Nations. Results on the referendum for independence, held on 1 March 1992, were not accepted by the Bosnian Serb leader at the time, since Serbs did not vote and it led to the declaration of Bosnia's independence, with two thirds of voters, excluding Bosnian Serbs. Not long after the United States and the European Union accepted Bosnia's independence, paramilitary forces were organized by the Bosnian Serbs. Those forces firstly attacked Sarajevo through bombarding the city with heavy artillery (Kulenović, 1998). The Yugoslav army, led by Serbian leader, joined the paramilitary forces in attacking multiple cities beside Sarajevo as the capital, such as Zvornik, Foča, Višegrad and many, many others in the east part of Bosnia.

War in Bosnia and Herzegovina ended with the assistance of the international community, by signing the General Framework Agreement for Peace in Dayton, initiated on 21 November 1995 and signed in Paris in December 1995. The aggression on Bosnia produced the biggest ethnical cleansing after the Holocaust, the Srebrenica genocide. In Srebrenica, more than 8372 Bosniak men and boys were killed while thousands of women were raped by the Bosnian Serbs and Serbian Serbs (Brunborg et al, 2005). Even after 28 years, the bones of many Srebrenica and Bosnia's war victims have not been found, due to the fact that the aggressors used mass graves to burry only parts of the killed civilians.

As part of the Dayton Peace Accords, the Constitution of Bosnia and Herzegovina divided this country into three administrative territorial units: Federation of Bosnia and Herzegovina with Bosniaks and Croats as majority; Republic of Srpska with Serbs as majority and Brčko District. Political representatives of the Republic of Srpska continued throughout all these years since the independence, to aspire for its own independence and to becoming part of the Republic of Serbia.

Political history of Ukraine

History of Ukraine, the same as Bosnia's, goes back in centuries, but we will mention the one going from the 13th century where Ukraine originates from the Kievan Rus, starting from the period of feudal fragmentation. In that period, the state was in a constant struggle for its independence, mainly with Turkey and Poland, but later on with Russia. Additionally, in the 18th century, Russia gained control over a big part of Ukraine.

Similar to Bosnia, after World War I, Russia became a republic of the Soviet Union with most of this territory, while the west part of Ukraine was divided among Czechoslovakia at the time, Romania and Poland. Stalin who at the time led the Soviet Union, in 1932 and 1933, caused Holodomor, death of many Ukrainians by starving to death.

Movements for independence in Ukraine were massive and in favor of the separation from the Soviet Union. One of the first forms of existence of the modern Ukrainian state goes back to the 1917 when there was the Ukrainian People's Republic.

Declaration of the State Sovereignty of Ukraine, enhanced in the 1990, had an impact on the status change of the Soviet Republic. The Supreme Court in the period that followed, adopted more legal acts and documents which led to the Ukrainian independence (Zhiltsov, 2020). In line with the adoption of the aforementioned documents, Ukraine faced a huge widespread movement for independence and rallies, to which the Soviet Union did not have any impact.

Again, as Bosnia, Ukraine was also divided via both regional and ethnic divisions. In the years that followed the independence, Ukraine was shaken by mass protests, such as the Orange Revolution and protest on the Kyiv's Maidan. Protests were seen as a vulnerability of Ukraine and a great opportunity to attack, which Russia took advantage of by starting the occupation of Crimea, a Ukrainian autonomous republic that was annexed by Russia after declaring its own independence. Eastern Ukraine, since 2014, has been under constant fight between pro-Russian separatists and the government of Ukraine.

As it can be seen from the above-stated, Bosnia and Ukraine share common historical battles for independence. Both were constantly under someone's watch, targeted and part of a larger community. After declaring independence, both were attacked by neighboring countries whose only objective was to conquer the newly-independent state and take away its independence and sovereignty.

NATO and EU and the War in Ukraine

Aggression on Ukraine has brought the foreign policy of many countries in the forefront, such as Hungary, Bulgarian, Turkey and even Romania. These countries at the beginning, showed pro-Russian orientation due to firstly, their dependence on the energy sources that Russia has, as well as its impact on the state institutions and domestic internal policies of these countries. Due to the aforementioned, Romania, Turkey, Hungary and Bulgaria were more cautious with respect to its foreign policy strategies. Unlike them, Greece announced at the very beginning that it will provide Ukraine with military assistance, as Jenkins (2023) stated.

While aggression on Ukraine was worsening, Sweden and Finland, whose military opinion was to be neutral for many, many years, decided that it would be in their best interest to join NATO. With this two new applications for membership and official attitudes by other NATO members, it became evident how the Alliance became ever more relevant.

In addition to strengthening NATO's relevance, Poland stepped up and showed support for Ukraine. As Poland was also victim of the Russia's big plans in the past, Poland's assistance to Ukraine was seen in the supply of weapons an route into Ukraine. Moreover, Poland gave home to 1.5 million Ukrainian refugees. Of course, Poland's assistance did not go without notice by Moscow where some allegations were made stating that Russia should prepare for a possible Polish invasion (Jenkins, 2023).

The European Union stands in solidarity with Ukraine and strongly condemns the brutal and aggressive invasion that Russia is doing against Ukraine, as well as the illegal annexation of Ukrainian provinces, as stated by the European Commission and the Council of the European Union. Additionally, the European Union raised its voice for the protection of Ukraine and its support was seen in imposing sanctions to Russia and its president Vladimir Putin, its associates and people of interest for the aggression as well as multiple requests that leaders of the EU stated to Russia to immediately stop its military operations and to unconditionally withdraw all forces, as well as military equipment from Ukraine. Doing so, EU requests that Russia respects the territorial integrity, sovereignty and independence of Ukraine. Furthermore, the European Union provided Ukraine with humanitarian, financial, military and political assistance, which was confirmed by Charles Michel, the President of the European Council in March 2023.

Moreover, the purpose of multiple sanctions that the EU imposed is to weaken the economic power that Russia has and hence, decrease its military power and ability. In total, the European Union imposed more than 10 different sanctions for Russia over a period of one year.

Connections between Russia and Serbia

Even during the 1990s, before Socialistic Federative Republic of Yugoslavia fell apart, it relied and depended on the Soviet Union when it comes to the armaments and weapons, mostly due to declining export markets of Yugoslavia. The mentioned support from the Soviet Union was seen in tanks, armored vehicles, ships and antiaircraft missiles, as stated by Sybir (2021).

As Sybrid mentions (2021), in Bosnia and Herzegovina, arms were supplied through the Third World Relief Agency, again with the support of the Soviet Union that actually made them and bought by various Eastern European countries.

Milošević, one of the aggressors during the war in Bosnia, had a brother, Borislav, whose political career at the time was based upon his ambassador job in Moscow. Due to this connection, Serbia was able to participate in the coordination of Russian mercenary recruitment and trafficking of different arms to their territory during the war. This thesis was also confirmed through the work of Ali (1999) where he mentioned how in that period, there was growing rage against NATO that resulted in the orientation to help Serbia, stating that NATO with its impact on Serbia, could introduce a new war in Central Europe.

In 2023, Serbia still has strong relations with Russia, even though those are not seen as public and communicated to the world. The same scenario that happened with Bosnia and Herzegovina in the 1990s is now happening in Ukraine where country-aggressor of the communist Federation (at the time Serbia and now Russia) is using various means to spread its propaganda, mostly through language and religion, in order to activate troops in neighboring countries or territories and in that manner, try to succeed them on the “bigger” territory.

Russia and NATO

Even in 1999, Ali wrote about NATO and the possible Ukrainian membership, stating that Russia could think about creating its own security alliance due to which the Ukrainian connection with NATO, especially on the border between Poland and Ukraine, would directly confront with Russia's idea of a new security alliance.

Russia has throughout the years made clear that it has a negative attitude towards NATO. In line with the current aggression on Ukraine, it is notable how Russia is using propaganda towards NATO, stating how NATO threatens Russia and wants to occupy it. Even before the aggression started, as stated by the Deutsche Welle (2023), Russia used this kind of narrative in order to spread the false news about how the West is interfering in Ukraine. The aim of such disinformation is creating a perception of Russia as the one that is threatened, jeopardized, and attacked by Ukraine, hence it has to defend itself. As one of the justifications for the aggression, just a few days prior to first strike, Vladimir Putin announced how NATO is spreading and getting close to Russia's borders with its military infrastructure by spreading towards the East. One of the most wide-spread narratives that Russia uses is that people that are Russian-speaking in the self-proclaimed republics Donetsk and Luhansk, were tortured for years and were victims of genocide by the Ukrainians. Hence, it has to be stopped and Ukraine has to be stopped, according to Russia's president.

As the Deutsche Welle reported, Russia's propaganda and fake news in Russia's state media go all the way to the accusations that NATO sent troops and that those are actively involved in the war in Ukraine.

It can be seen that nowadays, Russia has influence in the ethnic divisions of Bosnian citizens and assists the process of Republika Srpska's militarization. By doing so, Russia directly slows down the Euro-Atlantic process of the entire Bosnia and Herzegovina. Moreover, Russia's support to Republika Srpska officials is not only noticeable as soft power, but also through meetings that current Russia's president Vladimir Putin held throughout the years with RS's politicians.

BiH and NATO

Bosnia and Herzegovina aspires to become a member of the European Union and NATO. This aspiration is seen as a positive reform in Bosnia and Herzegovina that can impact on the process of democratization. Bosnia currently has the status of a candidate for membership in the EU, while its officials still seek to address all recommendation from the 14 key priorities that need to be solved and accepted before its formal membership. In 2021, BiH was expected to receive EUR 552 million through the program of IPA II allocations, as research by Garding (2021) shows. By receiving this amount of money, Bosnia becomes EU's biggest source of foreign assistance.

Opinions of leading Bosnian politicians regarding membership in both the EU and NATO, but more for NATO, are quite divided and contradictory. As during the 1990s, Bosnian Croats and Bosniaks are in favor of NATO, while Bosnian Serbs, led by radical and separatist politicians, are against the NATO path. The reason why Bosnian Serbs are against its NATO membership is based upon NATO's resentment during the war in Bosnia. In addition, leaders from Republika Srpska have aspirations towards Serbia, and hence are aligning with Serbia's opinions. The official path of Bosnia towards NATO started back in 2006, when Bosnia joined NATO's Partnership for Peace through which in 2008, the Individual Partnership Action Plan was established. Just two years after, NATO mentioned that it will start with the Membership Action Plan (MAP). MAP is used as a program the purpose of which is to provide assistance to the members in their process of achieving membership requirements. For Bosnia, the most challenging requirement received by NATO is the re-registration of the defense system to state level, as currently it is on the entity level government. As per arguments above, politicians from Republika Srpska resisted ceding control to the state level. Regardless of not fulfilling NATO's requirements and in line with positive gesture, in 2018, foreign ministers of NATO decided to invite Bosnia to activate its MAP through submission of the Annual National Program, first of its kind. In response to this, just one year after, members of the National Assembly of Republika Srpska voted in favor of the resolution that supports military neutrality.

During the current Russian aggression on Ukraine, as per opinion of the analyst and Garding (2021) some Bosnian Serb nationalists even fought on the Russian side as pro-Russian combatants in Ukraine.

Impact of the United States of America in Bosnia's war

As Garding (2021) wrote, during the 1990s war, Bosnia and Herzegovina held connections with the United States that was notable in support of the US after BiH gained its independence. The afore-mentioned support was through leading NATO forces and airstrikes against Bosnian Serbs with deployment of 20,000 US troops. In the years that followed, the United States supported the aspirations of Bosnia and Herzegovina for its path towards both NATO and EU membership (Garding, 2021).

Since the US had an important role in Bosnia and Herzegovina, during the war, there was a strong pressure on the US policymakers to involve even more in resolving the war, since most of the support was relied on the European Union and United Nations. NATO, alongside with the US command, finally intervened in August and September of 1995, with air strikes aimed at Bosnian Serbs. In addition to NATO's intervention in 1995, the role of the US was seen also with the 1994 Washington Agreement that ended the conflict between Bosniaks and Croats, the Dayton Peace Accords was signed at the Wright-Patterson Air Force base in Dayton, Ohio and also the US diplomat Richard Holbrooke was part of the brokering team for the General Framework Agreement for Peace (Garding, 2021).

Conclusion

As it was stated in this paper, Bosnia and Herzegovina and Ukraine have a lot of similarities. Firstly, both share a common historical origin by existing for centuries, but never as independent states until 1990s, always as part of another, greater force.

Even though war in Bosnia ended with pressure of the international community and resulted in the Dayton Peace Accords, the international community continues to play a significant role in shaping Bosnia's political system, even after 30 years. The impact of the international community in Bosnia is evident through the representation of the Office of the High Representative in Bosnia and Herzegovina that has jurisdiction to pass laws, above other. Additionally, there is an impact by Russia through its soft power, energy, and orientation towards Republika Srpska (entity where Serbs and Orthodox are the majority). Moreover, Turkish soft power is most notable in the religious tradition with Bosniaks and Muslims and the era of Ottoman heritage. Furthermore, China also has presence not only in Bosnia and Herzegovina but in the entire region (Garding, 2021).

In terms of Ukraine, the presence of the international community is evident – from support to non-support during Russia's aggression. Members of the international community decided to provide assistance to Ukraine, while some of them remained neutral and did not want to intervene between the two.

In comparison between aggression on Ukraine and aggression on Bosnia, a lot of similarities can be found:

- Both aggressions started when neighboring country, bigger forces, decided that they wants to enlarge their territory, hence strength and power;
- Both countries had separatist individuals and territories with separatist aspirations;
- Both countries are on its path towards the EU and NATO;
- There was a reaction by the international community in terms of protection.

REFERENCES:

Ademović, N., Steiner, C (2010). Constitution of Bosnia and Herzegovina, Commentary. Konrad Adenauer Stifund e.V. Rule of Law Program South East Europe Sarajevo

Ali, T., 1999. NATO's Balkan Adventure. *Monthly review (New York. 1949),* [online] 51(2), pp.9–14. https://doi.org/10.14452/MR-051-02-1999-06_2.

Anon 2021. NATO 2030. Brookings Institution Press.

Arapović, A (2012). Izborni sistem Bosne i Hercegovine: kritična analizra i komplikacija izbornog zakonodavstva. Tuzla: Centri civilnih inicijativa

Bajramović, Z., 2008. Evropska unija i izgradnja mira u Bosni i Hercegovini – vanjska percepcija. Godišnjak Fakulteta političkih nauka, (3–4), pp.390–398.

Garding, S.E., 2021. BOSNIA AND HERZEGOVINA: BACKGROUND AND U.S. POLICY. Current politics and economics of Russia, Eastern and Central Europe, 36(1), pp.1–4

Ibrahimagić, O (2009). Državnopravni i politički razvitak Bosne i Heercegovine. Autor: Sarajevo

Jacoby, W., 2010. The enlargement of the European Union and NATO : ordering from the menu in Central Europe. [online] International Bibliography of the Social Sciences (IBSS). Cambridge University Press. https://doi.org/10.1017/CBO9780511756221.

Jenkins, B.M., 2023. Consequences of the War in Ukraine: NATO's Future, commentary. RAND [online]. Available at https://www.rand.org/blog/2023/03/consequences-of-the-war-in-ukraine-natos-future.html

Kulenović, T (1998). Pripreme za rat i početak rata u Bosni i Hercegovini 1992 godine. UDK 355.4/479.6

Pejanović, M (20174). The State of Bosnia and Herzegovina and Democracy. Sarajevo: University Press

Schimmelfennig, F., 2009. The EU, NATO and the Integration of Europe. [online] International Bibliography of the Social Sciences (IBSS). Cambridge University Press. https://doi.org/10.1017/CBO9780511492068.

Šehić, Z., 2007. Bosna i Hercegovina 1992-1995 i međunarodna diplomatija. Posebna izdanja Akademije nauka i umjetnosti BiH, (37), pp.377–400.

Sybir, Viktoriia. What Was Military Cooperation Between Yugoslavia – The Soviet Union/Russia and How Was It Reflected During the Balkan Wars in the Nineties? The University of North Carolina at Chapel Hill ProQuest Dissertations Publishing, 2021. 28490009.

Zhiltsov, S.S., 2020. Ukraine. Nova Science Publishers, Incorporated.

Scientific article
UDK 355.02:[327:911.3(100)
UDK 004.8:[327:911.3(100)

ARTIFICIAL INTELLIGENCE: GEOPOLITICAL TOOL OF MODERN COUNTRIES

Stojanche MASEVSKI[1]
Slobodan STOJANOVSKI[2]

Abstract: *In this digitalized era, the geopolitical landscape has never been more uncertain. Political upheaval, social unrest and economic turmoil can spell disaster for every country. Modern countries don't have a lot of time to react to disasters when they occur.*

Artificial intelligence is the future of the world. Whoever becomes leader in its development usage is predestinated to rule the world. Artificial intelligence includes technologies like machine learning, intelligent robotics, biometrics, computer vision, swarm intelligence, natural language processing, virtual agents, semantic technology and natural language processing.

The rapid progress of artificial intelligence makes it a powerful tool from the economic, political, and military standpoints for modern states. With its implementation they can achieve their geopolitical and geoeconomic goals, and furthermore, they can change the foundations of international relationships. Artificial intelligence has become an instrument of power beyond our imaginations. Its usage will contribute to tectonic changes in geopolitics and in shaping the security of modern states.

So, if a modern state wants to fit into the digital age of humanity, and subsequently survive in it, instead of fighting frantically, it is inevitable that it will use artificial intelligence to achieve its goals.

Key words: *artificial intelligence, geopolitics, security, goals.*

Introduction

In this future world, increasingly divided along demographic, economic and technological lines, achieving human security will not be without its difficulties. Systemic challenges, such as climate change and war, and more localized threats like social, economic or political disruptions are almost certain. One way to meet these challenges is through novel applications of technology, and of AI in particular. AI holds much promise to enable the international community, governments and civil society to predict and prevent human insecurity. With increased connectivity, more sophisticated sensor data and better algorithms, AI applications may prove beneficial in securing basic needs and alleviating or stopping violent action (Roff, 2018, p.19). Information geopolitics cuts across all aspects of the economy, society and state security apparatus (Rosenbach and Mansted, 2019, p.16). The rapid progress of AI makes it a powerful tool from the economic, political, and military standpoints. Embedded in the digital revolution, AI will help determine the international order for decades to come, accen¬tuating and

[1] PhD student at the Institute for Security, Defense and Peace-Faculty of Philosophy Skopje
[2] PhD student at the Faculty of Security- Skopje

accelerating the dynamics of an old cycle in which technology and power reinforce one another. It will transform certain axioms of geo¬politics through new relations between territories, space-time dimensions, and immateriality (Miailhe, 2018, p. 105-117).

AI is key to the control of geographic space and the five dimensions (land, sea, air, space and cyber) of warfare and their interoperability. Recent developments in artificial intelligence (AI) suggest that this emerging technology will have a deterministic and potentially transformative influence on military power, strategic competition, and world politics more broadly.

These new geopolitical dynamics will be shaped by open rivalry over who can control and mitigate the power, failures and externalities of AI and converging technologies (Pauwels, 2019, p. 34). The advent of artificial intelligence promises to disrupt the realms of national security, geopolitical interaction, and international competition. In much the same way as these technologies, the power of artificial intelligence in augmenting human innovative and data-processing capabilities will allow states to expand their effectiveness in military, economic, and informational operations greatly, necessitating the adoption of this new technology in the crafting of 21st-century national strategies (Laverick, 2022, p.7).

Artificial intelligence

Given the complexity of the matter, a working definition of AI is needed. There is no one commonly agreed definition, even among computer scientists and engineers, but a general definition of AI is the capability of a computer system to perform tasks that normally require human intelligence, such as visual perception, speech recognition and decision-making. This definition is, however, inherently oversimplified, since what constitutes intelligent behavior is also open to debate. Arguably, by this definition a house thermostat is intelligent because it can perceive and adjust the temperature. This is substantially different from AI whereby a UAV selects and engages targets without meaningful human control, which is the common assumption for autonomous weapons (Cummings, 2018, p.7). AI is a sub-discipline of Cognitive Science; an interdisciplinary field of study that examines the mind and intelligence. AI is the study of how to create artificial systems that "think". These systems, known as "artificial agents", should be able to sense environmental variables, analyze them, and then make the best possible decision taking those variables into account (Stewart, 2015, p.2).

AI is the simulation of human intelligence, processed and exhibited by machines. The underlying idea is to enable computer systems to perform tasks in line with human intelligence, via a set of theories, methods, and algorithms, whereas cognitive computing is a subfield of AI and refers to computing that focuses on reasoning and understanding at a higher level. Computing is analogous to human cognition, rationale, and judgment. It has the capacity to deal with symbolic and conceptual information. It is receptive to different kinds of stimuli and is able to take accurate decisions in complex situations.

AI is propelled by the convergence and industrial maturity of three main techno-scientific tendencies: big data (the power to process enormous quantities of data, produced by the human internet and the Internet of Things), machine learning (the ability of computers to learn), and high-performance cloud computing. AI is an instrument of power right now, and it will be increasingly so as its applications develop, particularly in the military field. However, focusing exclusively on hard power would be a mistake, insofar as AI exercises indirect cultural, commercial, and political influence over its users around the world. This soft power, which especially benefits the American and Chinese digital empires, poses major problems of ethics and governance (Miailhe, 2018, p. 105-117).

We are entering an era of hybrid opportunities and threats generated by the combination of artificial intelligence (AI) and other powerful dual-use technologies, with implications for nearly every aspect of our daily lives. The convergence of AI and affective computing, cyber and biotechnologies, robotics and additive manufacturing raises complex global implications that are poorly understood, leaving the multilateral system with limited tools to anticipate and prevent emerging risks. At the same time, the spread of AI convergence across a wide range of States, non-State and transnational actors and entities means that the challenges of tomorrow must be addressed collectively and innovatively (Pauwels, 2019, p. 34).

Usages, benefits and challenges of artificial intelligence

AI has many uses in intelligence collection and analysis. For collection, the explosion of data that is occurring because of smart devices, the Internet of Things, and human internet activity is a tremendous source of potential information. This information would be impossible for humans to manually process and understand, but AI tools can help analyze connections between data, flag suspicious activity, spot trends, fuse disparate elements of data, map networks, and predict future behavior. This could make clandestine activity more challenging in a number of ways, as the combination of big data, data breaches, and increased open source information could make it more difficult to keep intelligence professionals undercover. For example, facial recognition and biometrics, combined with large surveillance systems, could make operating under aliases increasingly difficult. At the same time, AI systems may be vulnerable to counter-AI spoofing techniques, such as fooling images, which will have implications for the intelligence community. Deep fakes and the automation of data creation at scale may make it possible to create deep backstories for individuals undercover. AI may even transform verification of human reporting through improvements in systems that can correlate brain imaging to thoughts, with major implications for counter-intelligence and interrogation. AI also has tremendous potential value in intelligence analysis. AI systems can be used to track and analyze large amounts of data – including open-source data – at scale, looking for indications and warning of suspicious activity. Anomaly detection can help find terrorists, clandestine agents, or indications and warning of potential enemy military activity. AI based speech-to-text and translation services could greatly increase the scale of processing audio, video, and text-based foreign language information. AI systems could be used to generate simple automated reports, as they do already for some sports games (Horowitz, et al., 2018, p.11).

The role of AI in the shifting threat landscape has serious implications for information security, reflecting the broader impact of AI, through bots and related systems in the information age. AI's use can both exacerbate and mitigate the effects of disinformation within an evolving information ecosystem. Similar to the role of AI in cyber-attacks, AI provides mechanisms to narrowly tailor propaganda to a targeted audience, as well as increase its dissemination at scale – heightening its efficacy and reach. Alternatively, natural language understanding and other forms of machine learning can train computer models to detect and filter propaganda content and its amplifiers. Yet, too often the ability to create and spread disinformation outpaces AI-driven tools that detect it (Horowitz, et al., 2018, p.4-5). Robotic intelligence is likely to figure centrally in the crises, discontents, and conflicts of the future world system (Sham, 2017, p.454).

A clear majority of the responses from these experts contained material outlining certain challenges, fears or concerns about the AI-infused future. The five most-often mentioned concerns were: 1) the use of AI reduces individuals' control over their lives; 2) surveillance and data systems designed primarily for efficiency, profit and control are inherently dangerous; 3) displacement of human jobs by AI will widen economic and digital divides, possibly leading to social upheaval; 4) individuals' cognitive, social and survival skills will be diminished as they become dependent on AI; and 5) citizens will face increased vulnerabilities, such as exposure to cybercrime and cyberwarfare that spin out of control and the possibility that essential organizations are endangered by weaponized information. A few also worried about the wholesale destruction of humanity (Anderson, Rainie and Luchsinger, 2018, p.11).

Artificial intelligence and geopolitics

Throughout history, technology has transformed economies and societies, has redistributed (military) power among states, and has empowered new actors (Franke, 2021, p.13). The advent of artificial intelligence threatens to disrupt established geopolitical dynamics and facilitate a new dimension of competition between major international powers. In an article from 1997 entitled Internet géopolitise le monde, it was mentioned that "instead of making geopolitical conflicts more difficult to take place, the Internet seems to multiply and complicate them" the standard notions from the geopolitics field, such as power, influence and conflict are also "altered" by the new cyber dimension (Neascu and Chiciuc, 2021, p.165).

Previous researches suggests that geopolitics contains the essential elements of international relations, which can be influenced by social media as the activities of a country's political entity are public. Inappropriate use of social media, such as careless exchange of content might hurt public sentiments or affect deals. It is observed that political personalities of different nations often exchange words on social media platforms (Kamruzzaman, 2022, p.2). Social media is computer-mediated technologies with a huge amount of internet-based communication. Therefore, it generates a high risk for geopolitics and smooth economic growth from bad actors. AI and cognitive computing could help us mitigate those risks of social media. Following AI and cognitive computing tools can be used to address these issues. It is identified through the studies that geopolitics is impacted by social media through the users' ability. Politicians can use social media to influence individuals by using certain strategies. Two strategies have linked populism theory to a politician's ability to influence individuals through social media. The ability to influence individuals through social media by politicians has been categorized as unethical and bad practice by multiple studies as the situation may lead to a conflict of interest at a later stage. Furthermore, it is identified that social media has given rise to the spread of news that is troublesome for geopolitics as some governments or organizations like to preserve the ability to censor content for their own benefit. Another implication identified by social media on geopolitics is the number of protests caused by the platforms. However, it is important to note that an opposite effect also occurs, that is, in the case of less censorship, there is a greater development of social media (Kamruzzaman, 2022, p.9-11).

At the strategic level of decision-making, AI-enabled command and control systems will likely be able to avoid many shortcomings inherent to human strategic decision-making during the "fog of war" such as: the susceptibility to invest in sunk costs, skewed risk judgment, cognitive heuristics, and group-think. The U.S. intelligence community, for example, is actively pursuing several publicly documented AI research projects to reduce the "human-factors burden", increase actionable military intelligence, and enhance military decision-making, and ultimately, to predict future attacks and national security threats (Johnson, 2019, p. 4).

International humanitarian operations could also benefit greatly from AI technologies. AI technologies can help monitor elections, assist in peacekeeping operations, and ensure financial aid disbursements are not misused through anomaly detection. Of course, artificial intelligence can also help directly improve the quality of life in less developed nations by increasing productivity, health care, and myriad other economic benefits. Artificial intelligence could also help in avoiding disasters that lead to international intervention. For example, AI technologies that extract significant actionable warning signs from climate and soil patterns will be a boon in agricultural efficiency and disaster preparedness (Horowitz, et al., 2018, p.13).

Another set of roles for AI might be prediction rather than analysis. In other words, whereas analytical applications of AI are intended to streamline current operations, artificially intelligent systems may offer opportunities for policymakers to understand possible future events. One such example in the arena of international affairs would be the possibility of modelling complex negotiations. Along with using AI systems to monitor compliance and improve the efficiency of complex international instruments, parties to negotiations (whether economic or strategic in nature) might use machine-learning methods to forecast others' positions and tactics. It is worth noting, moreover, that AI might take on other predictive roles with a bearing on geopolitics, contributing for instance to more accurate forecasting of elections, economic performance and other relevant events. But such areas are functions less of machine learning and more of the quantity of data available, and so should instead be considered chiefly in that light (Parakilas and Bryce, 2018, p.3-4).

Cybergeopolitics is individualized as the newest geopolitical subbranch, which analyzes the movements of forces of global actors in the cyberspace, the motivations/ interests behind these movements and their impact on relations between actors in the global dynamic. In addition, cybergeopolitics can be used alongside cybergeostrategy to study the instruments of hybrid war. Cyberspace is the fifth dimension of geopolitics and geostrategy. The role of the geographical factor in maximizing power (control of land, seas and oceans, air, circumplanetary space) has been completed with a new dimension, the cybernetic one, which adds strengths in addition to the previous ones. Being a complex global network, based on interconnectivity and interdependence, cyberspace also presents vulnerabilities, which can be speculated to cause damage, including physical ones. In addition, the inexorable accessibility to the virtual space with minimal costs maximizes the number of potential geopolitical actors, state and non-state, other than the already established great powers (Neascu and Chiciuc, 2021, p.165).

Conclusion

First of all, the idea of collective security and alliances, the only formulas by which states can be able to withstand the current technological sprint. Secondly, a potential sliding towards a "techno-civilizational" global order, made by technological nomoses, meaning global technological regions. This new global configuration of technological nomoses attracts a large number of international actors, united by common interests, principles and values and, in case of confrontation, huge battlefields, massive forces engaged in battle, massive destructions and huge costs. Third, a new world order dictated by technological powers, which will be the future hegemons of the planet. A new world order which can take the current hegemonies out of the game, if they will not be able to keep up with the technological advance. A new world order which can bring to the fore other hegemonies – states or alliances (Popescu, 2021, p.14).

Of the countless forces that continue to shape the chaotic geopolitical landscape of the 21st century, there are none as simultaneously pervasive and impactful as the innovation of new and disruptive technologies. The maturation of the Information Age has forced some adaptation and evolution in our laws, regulations, and policies. But the pace and intensity of technological change has often made it difficult for the policy, regulations, and laws to keep up. As has been the case in other periods of intense change, the lag in the evolution of laws and regulations can lead to significant policy gaps (Osoba and Welser, 2017, p.2).

Artificial intelligence is the new weapon of states in achieving their goals at the international level. With its help, it is possible to act in almost all spheres of society (political, economic, military, sociological, ecological, etc.) and thereby strengthen one's own national security and at the same time force another state to submit to its demands.

Artificial intelligence is perceived as a geopolitical tools of modern states for several reasons. First, by measuring or monitoring geopolitical and geoeconomic events, pressures and trends, we can understand the geopolitical and geoeconomic reality. Secondly, with them we can more easily predict the future, that is, choose what steps or decisions we will choose. Third, by applying them, we will enable our national policy makers to create better national security, i.e. policy and strategy. Fourth, with their use we will gain a geopolitical and geoeconomic advantage over our neighbors, regional powers, and in some cases even over the great powers. Fifth, the application will affect the handling of geopolitical and geoeconomic pressures. Sixth, as an auxiliary tool, they play a major role in conducting international relations. Seventh, the application should give a positive result in the avoidance of geopolitical and geoeconomic risks or their mitigation, prevention, handling, i.e. management. Eighth, the artificial intelligence that will complete these procedures and functions can be objective, faster, more efficient and more effective than a certain expert in the field. Ninth, as an auxiliary tool in the formation of national security, it accelerates the process of making geopolitical and geoeconomic decisions. Tenth, their application provides a clear picture of the geopolitical and geoeconomic environment and the possibilities for a sudden deterioration of the geopolitical and geoeconomic climate.

It is important to realize that the ultimate goal of a respective regime or government – whether economic, geopolitical or societal, will be reflected by the way AI is used as a tool of governance or statecraft and must be understood through the perspective of intention. The application of AI as a tool of warfare clearly can be seen as a continuation of politics by digital means. Thus, AI must be viewed not only as the key component of the 4th Industrial Revolution but also as a revolution in warfare, which is commonly referred to as a "revolution in military affairs – RMA". Just as the bow and arrow were replaced by gunpowder and guns, AI will forever change how warfare is conducted (Fricke, 2020, p.2).

REFERENCES:

Anderson, J., Rainie, L., Luchsinger, A. (2018). *Artificial Intelligence and the Future of Humans*. Washington DC: Pew Research Center

Cummings, L. M. (2018). Artificial Intelligence and the Future of Warfare. *Chatham House Report*

Franke, U. (2021). *Artificial Intelligence diplomacy: Artificial Intelligence governance as a new European Union external policy tool*. Luxembourg: European Parliament, Department for Economic, Scientific and Quality of Life Policies

Fricke, B. (2020). *Artificial Intelligence, 5G and the Future Balance of Power*. Berlin: Konrad Adenauer Stiftung

Horowitz, C. M., Allen, C. G., Saravalle, E., Cho, A., Frederick, K. and Scharre, P. (2018). *Artificial Intelligence and International Security*. Washington DC: Center for a New American Security

Johnson, J. (2019). Artificial intelligence & future warfare: implications for international security. *Defense & Security Analysis*, 37(2)

Kamruzzaman, M.M. (2022). Impact of Social Media on Geopolitics and Economic Growth: Mitigating the Risks by Developing Artificial Intelligence and Cognitive Computing Tools. *Computational Intelligence and Neuroscience*, Vol. 2022

Laverick, R. (2022). *Artificial Intelligence and National Security*. Akron: Williams Honors College

Miailhe, N. (2018). The geopolitics of artificial intelligence: The return of empires?. *Politique étrangère*, 3

Neascu, C. M. and Chiciuc, A. I. (2021). Cyber geopolitics and cyber geostrategy- Emerging study fields. *STRATEGIES XXI: The Complex and Dynamic Nature of the Security Environment*

Osoba, A. O. and Welser, W. (2017). *The Risks of Artificial Intelligence to Security and the Future of Work*. Santa Monica: RAND Corporation

Parakilas, J. and Bryce, H. (2018). Introduction: Artificial Intelligence and International Politics. *Chatham House Report*

Pauwels, E. (2019). *The new geopolitics of converging risks: The UN and prevention in the era of AI*. New York: United Nations University Centre for Policy Research

Popescu, C. A. (2021). The geopolitical impact of the emerging technologies. *Bulletin of "Carol I" National Defence University*, 10(4)

Roff, M. H. (2018). Advancing Human Security Through Artificial Intelligence. *Chatham House Report*

Rosenbach, E. and Mansted, K. (2019). The Geopolitics of Information. *Belfer Center for Science and International Affairs*

Sham, G. I. (2017). Robot Wars: US Empire and geopolitics in the robotic age. *Security Dialogue*, 48(5)

Stewart, J. (2015). *Strong Artificial Intelligence and National Security: Operational and Strategic Implications*. Newport: Faculty of the Naval War College

CODE OF ETHICS

CONTEMPORARY MACEDONIAN DEFENCE is an international scientific journal published by the Ministry of Defence of the Republic of North Macedonia. The journal publishes scientific and professional articles by domestic and foreign authors that address topics in the field of defence, security and peace.

The Editorial Board of the jouirnal is guided by the highest professional and ethical standards, which means that plagiarism and other unacceptable forms of work in the academic community and in publishing are not tolerated.

All scientific articles published in the international scientific journal "Contemporary Macedonian Defence" are reviewed by relevant reviewers in the appropriate field of scientific research and are classified by the reviewers in several categories (original scientific article, scientific article and professional paper). Manuscripts are submitted to the reviewers in an anonymous form.

This Code of Ethics requires the authors of articles to use the sources correctly in the published articles, which means that they will fully list the sources and authors they have cited in their article. Ethics in the publishing of the articles implies that attention will be paid to hate speech and advocacy of discriminatory attitudes of any kind and on any basis, as well as to declaring any conflicts of interest.

All articles in which the authors do not adhere to this Code of Ethics will not be considered for publication in our scientific journal, which is decided at a meeting of the Editorial Board of the journal.

The authors are responsible for complying with the ethical and professional standards and must obtain approval from the authors for the transmission of portions of their texts or authorized video or other material if the author or the publisher so requests.

The International Scientific Journal "Contemporary Macedonian Defence" does not receive or publish articles that have already been published in another journal, or those in which there is a high degree of resemblance to an already published article of the particular author.

The citation in the articles must be consistent and in accordance with the rules set out in the Guidelines for Authors. At the end of the article there must be a section with reference literature in alphabetical order, listing the complete references.

The author should give due recognition to all those who contributed to the research. Those who have competently contributed to the research should be listed as co-authors. The first author, by submitting the manuscript, guarantees that all co-authors agree with the final version of the article and its final publication.

If the article is a research conducted on people (surveys, interviews, etc.), the author is obliged to provide information that the entire research process is conducted with consistent compliance with ethical standards to protect the safety, integrity and dignity of the research participants.

The reviewers are required to treat the manuscript in a confidential manner. The manuscript should not be disclosed or its contents discussed with anyone other than the editor or persons authorized by the editor. The reviewer is required to provide a brief explanation to the Editorial Board of his/her final decision regarding the manuscript, especially if the print decision is negative.

The reviewer is obliged to approach the review objectively. The feedback to the author (s) should be given as professionally as possible, without any personal attacks. The reviewer may not use for his / her own research any part of any data submitted to him / her in articles that are still not published. The reviewer is obliged to immediately inform the editor of any similarities between the manuscript under review and another paper, whether it has been published or is being reviewed by another journal. The reviewer must immediately notify the editor of a manuscript that contains plagiarism, falsified data, or views that constitute hate speech or reflect bias. In addition, the reviewer is obliged to make an objective assessment of whether he/she has sufficient competencies to review the submitted manuscript. If the assessment iis negative, he/she returns the manuscript to the editor / Editorial Board in the shortest possible term.

The editor should ensure that the submitted manuscripts are anonymous and should not disclose the names and other details of the reviewers to third parties without their permission.

The editor has the right to make the final decision on the acceptance or rejection of the manuscript, regarding the originality and clarity of the manuscript and its relevance to the journal. Under no circumstances should the editor engage in obliging the authors to cite the particular journal as a condition for accepting the manuscripts for publication.

The editor is responsible for timely review and should take reasonable steps if the author files a complaint with respect to the work of the reviewers.

CONTEMPORARY MACEDONIAN DEFENCE
INTERNATIONAL SCIENTIFIC JOURNAL

INSTRUCTIONS FOR AUTHORS

The magazine publishes only reviewed and specialized papers: original research papers, accompanying research papers and professional papers and book displays.

If Magazine accepts the paper the authors are not allowed to publish it in other journals.

Papers must not have more than one co-author.

The manuscript should be submitted in electronic form. The pages and appendices should be numbered.

Papers should be written in English, where the paper should have a title, abstract and keywords.

The paper which are not to be printed are returned to the authors with an explanation.

TECHNICAL SPECIFICATIONS OF THE PAPER

The paper should include: title, author, institution, abstract, keywords, introduction, main part, conclusion and reference. The full paper should not exceed 5000 words in English.

Title of the paper - 14 points, Times New Roman, centered. Title of the paper should be short, but give a true reflection of the content and preferably contain as many keywords from the subject matter covered as possible.

One blank line.

Authors name and surname, lower case (Bold), 11 points, Times New Roman, centered.

Two empty rows.

Institution – cursive (Italic), 11 points, Times New Roman, centered.

Two empty rows.

Abstract - 11 points, Times New Roman, single-spaced. The content of the abstract should be an essential and independent entity.

One blank line.

Keywords - maximum 5 words, 11 points, Times New Roman, single spaced.

Introduction - 11 points, Times New Roman, single-spaced. One blank line.

Main Part -11 points, Times New Roman, single-spaced.

One blank line.

Conclusion - 11 points, Times New Roman, single-spaced. The conclusion should be a brief summary of the paper, and to include research results that occurred.

One blank line.

Reference - 11 points, Times New Roman, cited according to the Harvard style of citation. The cited reference should be given in a separate chapter in the order in which they appear as footnotes in the text. Cite only the bibliographical data used in the text. Cite all types of sources of information - books, specialized magazines, websites, computer software, printed or e-mail correspondence, and even verbal conversation.

Papers that use tables, pictures, drawings, photographs, illustrations, graphs and schemes, should be numbered with Arabic numerals, and the title of the picture should be written underneath. Each image or group of images should be planned in a well structured manner. The images should be sent as separate JPG file with a minimum resolution of 300 dpi. Colour images are printed as black and white.

Format: A4-format, delivered in an electronic form.

Margins

TOP	5 cm	TOP	1.89”
BOTOOM	5 cm или Page Setup	BOTOOM	1.89”
LEFT	4 cm (inch)	LEFT	1.58”
RIGHT	4 cm	RIGHT	1.58”
		GUTTER	0”

The Editorial Board is obliged to submitt the papers to the competent reviewers. The reviewers and authors remain anonymous. The reviewed papers, together with any observations and opinions of the Editorial Board will be submitted to authors. They are obliged, within 15 days, to make the necessary corrections.

The time of publishing the paper, among other things, depends on following this guideline.

Deadlines for submission of papers - 30.03. and 31.10. in the current year

ADDRESS:

1. Prof.Dr. Marina Mitrevska –Editor in Chieve
   e-mail: marinamitrevska@yahoo.com

   or

2. Ass.prof. Zhanet Ristoska
   e-mail: zanet.ristovska @ morm.gov.mk
   zanet.ristoska@yahoo.com

   or

   sovremena@morm.gov.mk

MAGAZINE EDITORIAL BOARD
Skopje, 12.04.2018, ***Contemporary Macedonian Defence***

The magazine is published twice a year

www.mod.gov.mk/contemporary-macedonian-defense/

44

СОВРЕМЕНА CONTEMPORARY
МАКЕДОНСКА MACEDONIAN
ОДБРАНА DEFENCE

44

MICHEL FOUCHER, ANTOINE GARAPON

DRAŽEN BOŽOVIĆ

METODI HADJI-JANEV

NEVEN TRAJCHEVSKI, GOCE STEVANOSKI

NADICA TODOROVSKA, LJUPCHO SHOSHOLOVSKI

IGOR GJORESKI

IGOR GELEV, BILJANA POPOVSKA

EMINA MUŠIJA

STOJANCHE MASEVSKI, SLOBODAN STOJANOVSKI

СОВРЕМЕНА МАКЕДОНСКА ОДБРАНА