



Republic of Serbia
MINISTRY OF
FOREIGN AFFAIRS



FDB | FACULTY OF
DIPLOMACY
AND SECURITY

INTERNATIONAL SCIENTIFIC CONFERENCE



BINS 2024

SECURITY CHALLENGES OF
THE NEW WORLD

**CHALLENGES OF MILITARY NEUTRALITY
IN DYNAMIC GEOPOLITICAL RELATIONS**

CONFERENCE PROCEEDINGS

FACULTY OF DIPLOMACY AND SECURITY, BELGRADE

International scientific conference - BINS 2024

*CHALLENGES OF MILITARY NEUTRALITY
IN DYNAMIC GEOPOLITICAL RELATIONS*

CONFERENCE PROCEEDINGS

Faculty of Diplomacy and Security, Belgrade

CONFERENCE PROCEEDINGS

INTERNATIONAL SCIENTIFIC CONFERENCE - BINS 2024

CHALLENGES OF MILITARY NEUTRALITY IN DYNAMIC GEOPOLITICAL RELATIONS

Publisher:

Faculty of Diplomacy and Security
Milorada Ekmečića 2, Belgrade
www.fdb.edu.rs

For publisher:

Prof. Dr. Radojica Lazić

Editor:

Prof. Dr. Milica Bošković

Technical editor:

Branko Velov, MA

Cover:

Prof. Dr. Aleksandra Arvanitidis

Proofreading and translation:

Nataša Kankaraš

E-edition:

Faculty of Diplomacy and Security, Belgrade

Circulation:

100 copies

ISBN-978-86-87545-50-2

Belgrade, 2025

INTERNATIONAL SCIENTIFIC CONFERENCE - BINS 2024

CHALLENGES OF MILITARY NEUTRALITY IN DYNAMIC GEOPOLITICAL RELATIONS

FACULTY OF DIPLOMACY AND SECURITY
BELGRADE, MAY 22, 2024

Organizing Committee:

Prof. Dr. Radojica Lazić, Faculty of Diplomacy and Security, Belgrade
Prof. Dr. Milica Bošković, Faculty of Diplomacy and Security, Belgrade
Prof. Dr. Mihajlo Manić, Faculty of Diplomacy and Security, Belgrade
Prof. Dr. Aleksandra Arvanitidis, Faculty of Diplomacy and Security, Belgrade
Suzana Bošković-Prodanović, Ministry of Foreign Affairs of the Republic of Serbia
Doc. Dr. Predrag Đikanović, Ministry of Internal Affairs of the Republic of Serbia
Prof. Dr. Željko Brkić, Ministry of Internal Affairs of the Republic of Serbia
Prof. Dr. Momčilo Pavlović, Faculty of Diplomacy and Security, Belgrade
Prof. Dr. Saša Mijalković, University of Criminal Investigation and Police Studies, Serbia
Prof. Dr. Dragan Ranđelović, Faculty of Diplomacy and Security, Belgrade
Nemanja Stevanović, MA, Faculty of Diplomacy and Security, Belgrade

Scientific committee:

Prof. Dr. Žarko Braković, Faculty of Diplomacy and Security, Belgrade, Serbia
Doc. Dr. Danijela Bjelja, Faculty of Diplomacy and Security, Belgrade, Serbia
Doc. Dr. Katarina Šmakić, Faculty of Diplomacy and Security, Belgrade, Serbia
Prof. Dr. Ksenija Butorac, Police University College and University of Zagreb, Croatia
Prof. Dr. Emilia Alaverdova, David Agmashenebeli University of Georgia, Georgia
Prof. Dr. Tatyana Dronzina, Sofia University St. Kliment Ohridski, Bulgaria
Prof. Dr. Jovanka Šaranović, Strategic Research Institute, Serbia
Prof. Dr. Marija Đorić, Institute for Political Studies, Serbia
Prof. Dr. Bogdan Vukosavljević, European Research Institute for Strategic Studies, Slovenia
Prof. Dr. Goran Ilik, University St. Kliment Ohridski Bitola, North Macedonia
Prof. Dr. Piotr Pietrzak, Sofia University St. Kliment Ohridski, Bulgaria

CONTENT

FOREWORD	7
Radojica Lazić	
SUSTAINABILITY OF MILITARY NEUTRALITY OF THE REPUBLIC OF SERBIA IN MODERN GEOPOLITICAL CIRCUMSTANCES	8
Bogdana Koljević Griffith & Matthieu Grandpierron	
FORMS OF CONTEMPORARY CONFLICTS IN THE ERA OF THE END OF NEOLIBERALISM AND BIOPOLITICS	22
Brankica Janković	
MODERN APPROACHES TO SECURITY – FEMINIST THEORIES	33
Milica Bošković & Mina Suknović	
SOCIETAL SECURITY AT GLOBALIZATION – LANGUAGE AS TOOL AND OBJECT OF SECURITIZATION	47
Katarina Šmakić & Divna Vuksanović	
MEDIA AND NON-MILITARY THREATS IN HYBRID WARFARE: CAPTOLOGICAL TOOLS – PROBLEM-BASED APPROACH	56
Nemanja Stevanović & Dušan Radulović	
CYBER DEFENCE STRATEGIES OF MILITARY NEUTRAL COUNTRIES – CASE STUDY: SWITZERLAND	67
Hossam Nabil Elshenraky	
THE MODERN SECURITY STRATEGIES IN CONFRONTING CYBER PHISHING ATTACKS	83
Gordana Mišev, Andjelija Djukić & Miloš Tošić	
CHALLENGES OF MILITARY NEUTRALITY IN THE CONTEXT OF CONTEMPORARY GEOPOLITICAL RELATIONS IN EUROPE	109
Milan Miljković, Hatidža Beriša & Dejan Petrović	
CHARACTERISTICS OF MODERN CONFLICTS IN THE INFORMATION SPACE AND THEIR APPLICATION IN THE DETERRENCE STRATEGY	123
Hatidža Beriša, Dejan Petrović & Milan Miljković	
CHANGE OF MILITARY DOCTRINES IN THE RUSSIAN - UKRAINIAN WAR AS A FACTOR OF NEW TECHNOLOGIES	137
Miranda Gurgenedze & Tamazi Urtmelidze	
INTELLECTUAL PROPERTY IN GLOBAL SECURITY: BALANCING RIGHTS AND PROTECTION STRATEGIES	147

Caner Asbaş & Şule Erdem Tuzlukaya THE BRIDGE BETWEEN STRATEGIC MANAGEMENT SCHOOLS AND SECURITY STRATEGIES IN INTERNATIONAL RELATIONS: AN INTERDISCIPLINARY APPROACH	158
Şule Erdem Tuzlukaya RESERVE MILITARY FORCES OF NEUTRAL COUNTRIES AT MODERN CONFLICTS	175
Emilia Alaverdov, Nino Bochorishvili & Zurabi Tchabashvili THE IMPACT OF ILLEGAL MIGRATION ON TRAFFICKING AND ORGANIZED CRIME	190
Galit M. Ben THE CHANGING NATURE OF ARMED CONFLICTS IN THE 21ST CENTURY	199
Batya Brutin HOLOCAUST ICONS IN VISUAL ART AND THE ISRAELI- PALESTINIAN CONFLICT	215
Sanja Đurđević GLOBAL RISE OF VIOLENCE AND NARCISSISTIC CULTURE - WHERE IS THE WORLD HEADING?	228
Dejan Labović & Zoran Marjanović THE ROLE OF THE PRIVATE SECURITY SECTOR IN THE PREVENTION OF INTERSTATE CONFLICTS	243
Miriam Ugulava ISLAMIC FUNDAMENTALISM AND ITS ROLE IN POLITICIZING RELIGION	261
Vladan Borović & Stefana Matović ADVANCED SYSTEMS FOR REMOTE DETERMINATION OF THE POSITION OF MILITARY UNITS IN SPACE	273
Dragan Ranđelović CYBER SECURITY AS NON-MILITARY SECURITY RISK IN THE INFORMATION SOCIETY	291
Rejani Thudalikunnil Gopalan HUMAN TRAFFICKING: ENTRAPMENT METHODS AND FORENSIC INVESTIGATIONS	303

FOREWORD

The Challenges of Military Neutrality in Dynamic Geopolitical Relations Conference is the final activity of the project of the same name, which was carried out by the Faculty of Diplomacy and Security in cooperation with the Ministry of Foreign Affairs of the Republic of Serbia during 2023 and 2024. The aim was to present scientific papers on the topics of security, globalization, contemporary risks and strategic orientations, but also to discuss on relevant academic and experiential grounds. The Conference brought together a significant number of authors from the country and abroad, and we would like to thank them, as well as all the members of the Scientific and Organizational Committee of the Conference, for their engagement and effort so that this event, under the umbrella title *Security Challenges of the New World* (Bezbednosni Izazovi Novog Sveta – BINS), becomes a traditional annual event at our Faculty. The papers presented in this Collection represent the authors' current scientific and research contributions, as well as material for further research, but also education of students.

Editor

Prof. Dr. Milica Bošković
Vice Dean for Science and Research

*Radojica Lazić*¹

SUSTAINABILITY OF MILITARY NEUTRALITY OF THE REPUBLIC OF SERBIA IN MODERN GEOPOLITICAL CIRCUMSTANCES

Abstract

The military neutrality of the Republic of Serbia is being seriously tested amid the geopolitical changes that have occurred following Russia's special military operation in Ukraine. By addressing current global and regional developments, this research will attempt to prove the justification of such a policy and the positions expressed in the National Security Strategy. The paper primarily deals with the analysis and synthesis of current events in international relations and their impact on the position of the Republic of Serbia, through the prism of strategic orientations and military neutrality. At the same time, all relevant scientific sources and knowledge on this complex issue are studied, including a survey conducted among Serbian citizens on the sustainability of military neutrality.

Keywords: *Republic of Serbia, military neutrality, National Security Strategy, geopolitical changes, war in Ukraine.*

INTRODUCTORY CONSIDERATIONS

The strategic commitment of the Republic of Serbia in the field of security and defense policy implies that the highest legal acts define the basic interests of national security and what policy will be pursued in order to achieve them. The institutions of the security system must be ready to act at all times and to recognize any form of threat, and to try to thwart and neutralize it with their activities (Lazić, 2022: 73). For these reasons, there must be a structured way of management and subordination within the national security system. Its efficiency is conditioned by organization in achieving national security goals (Lazić, 2023: 18-21; Stajić, 2021: 55-65).

It took quite some time for all the important political and security factors to agree and decide that the highest legal act that comprehensively defines the interests of national security is precisely the National Security Strategy. It is true that the Constitution of the Republic of Serbia provided for the existence of the Defense Strategy (Ustav RS, 2006: Article 99, point 9), as the highest document in the field of defense, while there was no mention of the National Security Strategy. The doubt remains, which is present to this day, whether the framers of the Constitution intentionally or accidentally bypassed or

¹ Faculty of Diplomacy and Security, Belgrade, Serbia, e-mail: radojica.lazic@fdb.edu.rs

overlooked that important fact, and therefore gave primacy to the Defense Strategy, and not the National Security Strategy, in that highest legal act. The dilemma was resolved on October 26, 2009, when the National Assembly of the Republic of Serbia adopted both documents. The prevailing fact is that the National Security Strategy (NSS) is "the most important strategic document that establishes the foundations of security policy in protecting the national interests of the Republic of Serbia" (Strategija nacionalne bezbednosti, 2009: Introduction, paragraph 1). Its basic starting points relate to the preservation of sovereignty and territorial integrity, economic prosperity, social stability, the development of democracy, the rule of law, respect for human rights and freedoms, European foreign policy orientations, and the improvement of cooperation with the most important international entities and countries in the immediate environment. The Defense Strategy (DS) is "the basic strategic document that directs the engagement of defense resources and the development of normative, doctrinal and organizational solutions for the defense system of the Republic of Serbia" (Strategija odbrane, 2009: Introduction, paragraph 1). The Defense Strategy is "based on the Constitution of the Republic of Serbia, the National Security Strategy, as well as the commitment of the Republic of Serbia to contribute to building and strengthening security through peace and stability" (Strategija odbrane, 2009: Introduction, paragraph 2); Strategija odbrane, 2019: paragraph 3).

The basic commitments in the field of national security are therefore defined in the national security strategies of 2009 and 2019. The 2019 document, without further explanation, states as the basic starting points "preservation of sovereignty and territorial integrity, military neutrality, care for the Serbian people outside the borders of the Republic of Serbia, European integration and effective rule of law" (Strategija nacionalne bezbednosti, 2019: point 2, paragraph 2). The sustainability of military neutrality is, precisely, the topic of this paper. It should show to what extent and whether the military neutrality proclaimed on December 26, 2007 in the Resolution of the National Assembly on the Protection of the Sovereignty, Territorial Integrity and Constitutional Order of the Republic of Serbia is sustainable at all (Rezolucija Narodne skupštine Republike Srbije o zaštiti suvereniteta, teritorijalnog integriteta i ustavnog poretka Republike Srbije, 2007). In order to provide a comprehensive and concrete answer to this question, we have comprehensively analyzed, through various examples, the concepts of military neutrality, as well as relations between states and political developments on the international stage, as well as changes that have occurred on the global level. Of course, an inevitable topic in this comprehensive research is European integration, relations with the EU, the USA, Russia and China, as well as the position of our southern province of Kosovo and Metohija. The status of the Republika Srpska in Bosnia and Herzegovina, as a dysfunctional state and the aspirations of some of the most powerful countries to once again achieve majoritarianism and disrespect for everything that was agreed upon

in Dayton in 1995, is also unavoidable.²

In order to comprehensively examine attitudes towards military neutrality in Serbia, which is still a topic of serious political and professional debate, fourth-year undergraduate students at the Faculty of Diplomacy and Security surveyed 562 people of different ages.³ In this way, we learned what the citizens of the Republic of Serbia think about this issue.⁴

Neutrality in the practice of European states

In order to have a more comprehensive view of the phenomenon of neutrality, what it entails and how it affects the state and its position in international relations, we started from theoretical and practical points of view. In addition, it is important to study and compare different examples and practices, how and in what way different states implement them, and whether there are certain legal, internationally codified documents in this area that are applied.

From a conceptual perspective, the word neutrality comes from the Latin word *neuter*, which means "neither one nor the other", that is, to remain neutral and be "for neither side" in any relationship. In a practical sense, neutrality appeared at the beginning of the sixteenth century, only to be fully accepted in the nineteenth century (Jovanović, 2019: 1212). However, ever since states and their relations have existed, this concept has had its application, especially in wars. We find such examples as far back as the period of Ancient Greece and the Peloponnesian Wars, where one side offered its military neutrality (the Melians) in the conflict between Athens and Sparta (Tukidid, 1957: 316, point 95).

From the perspective of international law, the neutrality of a state first appeared in 1815, based on the decision of the Congress of Vienna. Such a status was recognized for Switzerland. It was not until the beginning of the twentieth century that an official document "relating to the legal status of neutral states in the event of a specific war conflict was created: the Hague Convention V on the Rights and Obligations of Neutral States in the Event of War on Land of 1907" (Novaković, 2019: 31). Although, from

² *The General Framework Agreement for Peace in Bosnia and Herzegovina*, better known as the *Dayton Peace Agreement*, is an international legal act that ended the three-year civil war in Bosnia and Herzegovina. Based on this agreement, Bosnia and Herzegovina consists of two entities: the Federation of Bosnia and Herzegovina and the Republika Srpska. It was reached and agreed upon at the US Wright-Peterson Air Force Base near Dayton, following a peace conference held from 1 to 21 November 1995. The participants were: Slobodan Milošević, President of the Republic of Serbia, Alija Izetbegović, Chairman of the Presidency of Bosnia and Herzegovina, Franjo Tuđman, President of Croatia, Warren Christopher, US Secretary of State, Richard Holbrooke and General Wesley Clark. It was officially signed on 14 November 1995 in Paris.

³ Fourth-year undergraduate students at the Faculty of Diplomacy and Security participated in the design of survey questions within the National Security Strategy course. The research was conducted by Elena Memiši and Dejan Gojsović.

⁴ The research results will be presented at the end of this paper.

the current point of view, this document is outdated, it represents the backbone of neutrality in war conflicts between states (Novaković, 2012: 4). The basic provisions of this document relate to the rights and obligations of neutral states. The most significant are the following: the territory of neutral powers is inviolable; the belligerents are prohibited from passing their troops or convoys, whether with ammunition or supplies, through the territory of a neutral power; the belligerents are prohibited: a) from installing a radio-telegraph station or any other device intended to serve as a means of communication with the belligerents on land or at sea in the territory of a neutral power; b) from using any device of this kind which they have established before the war in the territory of a neutral power for exclusively military purposes, and which was not open to public postal traffic; that no combat units may be established in the territory of a neutral power for the benefit of the belligerents, nor may recruiting offices be opened; a neutral power is obliged to punish acts contrary to neutrality only if they are committed in its own territory (Peta Haška konvencija, 1907).

The same Convention defined that if citizens of a neutral state voluntarily enter the service of one of the belligerents, such activity does not give rise to the responsibility of the neutral state. In addition, a neutral state was not obliged to prevent the export or transit to one or the other belligerent party of arms and ammunition, as well as anything else that would be of use to the belligerent parties.

In addition to the above, the Thirteenth Hague Convention on the Rights and Duties of Neutral States in Naval War, adopted on October 18, 1907 in The Hague, defined the relationship of neutral powers at sea. Based on this document, the belligerent parties were obliged to respect the sovereign rights of neutral states and to refrain, on land and on water, from acts that would, for the state that would tolerate them, constitute a violation of its neutrality. All hostile acts, including stoppages and searches, carried out by warships of belligerents in the territorial sea of a neutral state constituted a violation of neutrality and were expressly prohibited. Also, a belligerent could not establish a maritime spoils court on neutral land or on board a ship in neutral waters (Trinaesta Haška konvencija, 1907). Smilja Avramov and Milenko Kreća are of the opinion that "neutrality gives rise to reciprocal rights and obligations, both of the state in conflict, and of third parties and states that have declared neutrality" (Avramov & Kreća, 2003: 718). The concept of neutrality can basically be reduced to the state remaining impartial and outside of armed conflicts, that is, not participating in the hostilities of other states that are at war (Stojanović, Šaranović, 2022. 14).

Apart from Switzerland, whose military neutrality dates back to the sixteenth century, and which it officially acquired at the Congress of Vienna in 1815 and has retained until the present time, the following states were considered military neutral in

the second half of the twentieth century, and after World War II: Austria⁵, Ireland⁶, Finland⁷, Sweden⁸ and Malta⁹. When we talk about military neutrality, "it can be the result of an independent and sovereign decision of a certain state, as is the case with Switzerland, Sweden or Ireland, and it can also be strongly suggested, that is, imposed from the outside, as in the case of Finland and Austria" (Jovanović, 2019: 1223).

Austria has established its neutrality in the Constitution, as a permanent commitment, but, like Ireland, has joined the economic sanctions against Russia due to the special military operation in Ukraine. Finland and Sweden, during 2023, or early 2024, became full members of the NATO alliance.

NATO expansion and the Ukrainian Crisis

International relations, after the end of World War II, were for many years characterized by a "balance of power" and bipolarity in the field of security (Simić, 2002: 17; Stajić & Lazić, 2015: 31-32; Proroković, 2023: 47). This meant that the world divided into blocs between the world's largest powers, that is, between the ideological rivals of the East (communism) and the West (capitalism), was, at least to some extent, balanced. With the fall of the Berlin Wall, the collapse of the Soviet Union and the Warsaw Pact, the wars in the former SFRY and the formation of new states, a unipolar world order was established with one most powerful superpower (the USA) and the NATO alliance (Stajić & Lazić, 2015: 32). It has welcomed 16 more countries under its umbrella, including 7 March 2024 and the accession of Sweden.¹⁰

⁵ The 1955 State Treaty, which is still in force, excludes the possibility of Austria's military intervention in the conflicts of other countries, the stationing of foreign troops on its territory, and joining any military alliance.

⁶ Ireland declared its neutrality in 1938. It has maintained this status throughout and after World War II, and continues to this day. As a member of the EU since 1973, it has remained militarily neutral in relation to the war in Ukraine.

⁷ It concluded a friendship treaty with the Soviet Union in 1948, when its neutrality began. With the collapse of the USSR, the treaty was annulled. Finland became a member of the EU in 1995, and from 2023, upon joining NATO, it will cease to be a militarily neutral state.

⁸ It is one of the few countries that has been militarily neutral for almost two centuries. It has called its own policy "non-aligned in peacetime, neutral in wartime". By joining NATO in March 2024, it will end its neutrality.

⁹ Malta declared military neutrality in 1980, which was guaranteed in an agreement with Italy in 1983.

¹⁰ After the collapse of the USSR and the Warsaw Pact, the NATO Pact accepted all the countries that belonged to that alliance into its membership, including the three Baltic states from the former USSR (Estonia, Latvia and Lithuania). The accelerated process of joining under the NATO umbrella has included four new states that emerged from the collapse of the SFRY, except for Bosnia and Herzegovina and Serbia. Incidentally, the Muslim-Croat Federation as an entity of Bosnia and Herzegovina insists on joining NATO, while the Serbian member in the collective Presidency of Bosnia and Herzegovina is explicitly against it. In addition to the 32 members, 21 more countries cooperate with NATO within the Partnership for Peace program, including the Republic of Serbia.

Although, at the very beginning, after the disappearance of the Soviet Union, the highest officials of that military-political structure said that it would not expand and accept new members, the promise was not kept. During that period, NATO admitted: Poland, Estonia, Latvia, Lithuania, the Czech Republic, Slovakia, Hungary, Bulgaria, Romania, Slovenia, Albania, Croatia, Montenegro, North Macedonia, and recently Finland and Sweden, which until recently were considered neutral states.

It did not stop there. The Ukrainian crisis, which began with a colored revolution and a violent change of power in that country, supported by secret forces from outside, was a serious announcement that the NATO alliance and the USA had resolutely set out to conquer new space, approaching Russia at a critical distance. It is obvious that the Minsk agreements¹¹ were just a "bluff" to buy the other side time to better prepare for what came later, which was war.

It is worth noting that certain processes that took place before that seriously hinted that in the coming period, within the framework of the "bifurcation in the redistribution of new power" among the most powerful powers of the world, some kind of agreement on spheres and zones of influence would have to be reached. The changes taking place on the global level tell us that a number of economically strong states do not recognize and do not want the universal power of one alliance or one state, as the largest superpower. They insist on multipolarity in international relations and strive to create such an order, in which there would be several powerful centers in different parts of the world.

The war in Ukraine and the special military operation, as defined by the highest Russian officials, caused tectonic changes on the geopolitical plane and in international relations. The collective West got involved in this conflict, supporting Ukraine with weapons and financial resources. Various types of sanctions were imposed on Russia.¹²

Security challenges and military neutrality of Serbia

In scientific, expert and political circles, there have been discussions for a long time about whether the Republic of Serbia should be and whether and for how long it will be able to remain militarily neutral, given international relations and political developments in the world. Recently, due to the worsening political and security situation resulting from the "special military operation of Russia in Ukraine", the question has been raised more and more often as to the extent to which, or whether, the military neutrality proclaimed at the end of December 2007 by the Resolution of the National Assembly on the Protection of the Sovereignty, Territorial Integrity and Constitutional

¹¹ *The Minsk Protocol* is a document signed on 5 September 2014, which agreed to a ceasefire in the Donetsk and Luhansk regions of Ukraine. Despite the protocol, hostilities have continued. An updated version of the document, known as the Minsk 2 Agreement, was signed on 12 February 2015.

¹² On January 23, 2024, the European Union introduced the thirteenth package of sanctions against Russia.

Order of the Republic of Serbia is sustainable. Point 6 of the aforementioned Resolution states: "Due to the overall role of the NATO Pact, from the illegal bombing of Serbia in 1999 without a decision of the Security Council, to Annex 11 of the rejected Ahtisaari Plan, which stipulates that NATO is the 'final authority' in 'independent Kosovo', the National Assembly of the Republic of Serbia hereby decides to declare military neutrality in relation to existing military alliances, pending the possible calling of a referendum, at which a final decision on this issue would be made."

The Republic of Serbia, faced with new security challenges, risks and threats to national security, and in order to preserve the highest vital values, adopted the aforementioned Resolution on Military Neutrality. The reason for its adoption is quite clear, when, against its will, decisions were being prepared on the self-proclaiming and recognition of the independence of our southern province (Kosovo and Metohija) by the most powerful Western states. In such circumstances, there were neither the conditions nor the time to conduct a debate or referendum on the issue.

Although the National Assembly of the Republic of Serbia voted for military neutrality by the will of the majority of MPs, there was no clear consensus in the broader social sense regarding its acceptance. The Government of Prime Minister Mirko Cvetković¹³ did not address the issue seriously either, which is why the National Security Strategy from October 2009 does not mention the military neutrality of our country, nor the Atlantic, but only the European integration.

The aforementioned changes have led to the Republic of Serbia, as a sovereign state, having the need to remain militarily neutral. At the same time, it "achieves cooperation through a partnership with NATO, through membership in the Partnership for Peace Program, develops military cooperation with the Russian Federation, and in the military structure of the former Soviet states, the Collective Security Treaty Organization (CSTO), it has observer status" (Krga, 2017: 56). In this sense, it emphasizes that it will conduct a balanced foreign policy, cooperating with everyone, relying on four pillars (EU, Russia, China, USA), taking into account its priorities and national security interests. Serbia's foreign policy priorities in relation to European integration have remained the same – full membership in the EU. Such a commitment in no way threatens its military neutrality.

Quite understandably, the question arises whether EU membership is achievable or just a fiction, because most member states have recognized the independence of our southern autonomous province. One of the key conditions for Serbia's entry into the EU is the normalization of relations with Priština, i.e., recognition of independence. In addition, Serbia is also obliged to harmonize its foreign policy with EU policy by the end of the opening of the chapters (now the clusters). In the current circumstances, this would mean the introduction of sanctions against Russia, which is unacceptable for our

¹³ The deputies of the National Assembly of the Republic of Serbia, at a session held on 7 July 2008, voted in a new Government, with Prime Minister Mirko Cvetković. It functioned for a full four-year mandate.

country. Therefore, Serbia's European prospects, in the current circumstances, and this is clear to everyone, are completely uncertain.

At the same time, talks on the normalization of relations between Belgrade and Priština under the patronage of the EU have been at a standstill for a long time. The implementation of the agreements signed back in 2013 and the formation of the Community of Serbian Municipalities are being persistently avoided. The interim authorities in Priština are taking unilateral steps that are not in line with the agreements reached. The mediators in the negotiations and the international community are silent or giving lukewarm statements encouraging Priština to continue in this direction. Such steps were taken by voting for the admission of the so-called state of Kosovo to the Council of Europe. Ignoring the opposition of Serbia and some other countries, this decision received an overwhelming majority in the Parliamentary Assembly of the Council of Europe. However, it did not receive the "green light" from the Council of Ministers, which makes the final decision.

In addition, the adopted Resolution on the Srebrenica genocide, submitted to the UN General Assembly by Germany and Rwanda,¹⁴ further complicated Serbia's international position. The Resolution represents a flagrant example of the violation of all international legal norms and the undermining of the Dayton Agreement, which brought the peoples of Bosnia and Herzegovina a more or less guaranteed peace, but a dysfunctional state with two entities and three peoples who must agree on the most important matters by consensus. By putting the genocidal stamp on one people, the achieved peace is violated and new divisions and frictions are encouraged in Bosnia and Herzegovina.

On the global level, in the changed political and security circumstances, consistent implementation of the policy of military neutrality allows Serbia to reduce the pressure of Western countries to recognize Kosovo's independence, while simultaneously developing economic cooperation, both with them and with other significant actors such as Russia and China. Serbia's European integration perspective with the conflict in Ukraine becomes "extremely out of place, and the strategy of neutral, balancing maneuvering, although difficult and resembling 'walking a tightrope' is growing into a vital imperative for Serbia. Regardless of the fact that it means facing a whole range of combined provocations and pressures, the compliance with which inevitably leads to a losing 'comprehensive arrangement' under the guise of compromise, giving in means surrendering and drowning in a camp that is weakening in global relations and, at the same time, constantly defending its positions in the Balkans, feeding itself to the detriment of Serbian interests" (Gajić, 2023: 69-70).

¹⁴ *United Nations General Assembly Resolution 78/282* was adopted on 23 May 2024 at the 78th session of the United Nations General Assembly. The resolution was proposed by Germany and Rwanda, with the support of about thirty other states. Of the total number of United Nations member states (193), 84 voted in favor of the proposed text of the Resolution, while 19 states voted against, 68 abstained, and the remaining 22 states did not participate in the vote.

In an unfavorable strategic environment, military neutrality, as a foreign policy orientation, influences the creation of a positive image of Serbia as a reliable partner of the great powers (Forca, 2022: 182). This contributes not only to the strengthening and protection of its security, but also to a more favorable economic environment. On the other hand, military neutrality was created and has remained as such to this day, and it is assumed that it will remain so in the coming period, as a clear response to non-military threats to which it is permanently exposed by Western countries. In the coming period, they will be directed at achieving the interests of those countries. The goal is to weaken Serbia's position and to force it to do what those countries expect of it. Only through well-thought-out political action and principled positions can we demonstrate to both sides that the Republic of Serbia, with its principled position on military neutrality, does not endanger anyone. There are divided opinions about the feasibility of Serbia's military neutrality in the current geopolitical circumstances, and we must decide which side we will take. Some believe that it means nothing if it is not internationally recognized by the most powerful states, while others believe that it is a political decision of the state that declared it. For example, Aleksandar Gajić is of the opinion that "the only real and meaningful alternative (in the current circumstances) is to continue to persist in the current position, because only in this way can we exist in the long term, even at the cost of Serbia being a "lonely island" for a while until the international situation changes permanently to its multipolar dimensions" (Gajić, 2023: 70). On the other hand, Ljubiša Despotović and Vanja Glišin advocate "a clearer, more predictable and comprehensive definition of the priorities of national goals and national interests" (Despotović & Glišin, 2021: 29) and propose the adoption of a new national security strategy. They believe that this could "determine vital national interests as well as the next steps in foreign policy that will effectively and for a longer period protect the state of Serbia and the Serbian people as a whole" (Despotović & Glišin, 2021: 33).

CONCLUSION

Based on the above, as well as the research conducted, the conclusion is that the Republic of Serbia remains consistent with the policy of military neutrality. It should persist in this until the processes initiated on the global level are completed. They will be completed when the most powerful actors reach an agreement on the most important international issues in shaping the new world order. Undoubtedly, European integration remains a vague prospect for Serbia, but, nevertheless, at least declaratively, we should strive towards them. Within the framework of foreign policy tasks, there remains the raising of bilateral relations with the USA to a higher level; strengthening partnership ties with China; continuing good relations with Russia, without introducing sanctions; respecting the territorial sovereignty and integrity of Ukraine; continuing negotiations

with Priština, while insisting on the implementation of the agreement reached on the formation of the Community of Serbian Municipalities; strengthening the security and defense capacities of our country and deterring any type of aggression.

It should continue to balance in the coming period with wise and, above all, co-existing political decisions. It is estimated that in the near future there will be inevitable changes in relations between the great powers. This also implies new divisions of spheres of interest on the global level, after the conflict in Ukraine has stopped. It is expected that all this could contribute to a greater degree of understanding for our political position and the problems we are solving.

The reactions of Western countries, including EU members, after the end of the war in Ukraine, will continue to be aimed at completely neutralizing the influence of Russia and China in the European space, and especially in the Western Balkans, where their main focus is the Republic of Serbia. In such circumstances, Serbia should more clearly define its position of military neutrality and have it, in some way, recognized and confirmed by at least a certain number of countries. In addition, in the newly emerging geopolitical circumstances, there is a need to amend strategic and doctrinal documents, which would more precisely define Serbia's position and new realities in protecting national security interests. These documents would strengthen the position of the Republic of Serbia in protecting national and vital values, including military neutrality as a strategic commitment.

REFERENCE LIST

Avramov, S. & Kreća, R. (2003). *Međunarodno javno pravo*. Beograd: Savremena administracija.

Despotović, Lj. & Glišin, V. (2021). Geopolitički identitet Republike Srbije i Strategija nacionalne bezbednosti. *Politika nacionalne bezbednosti*, 1, 21-35.

Forca, B. (2022). Vojna neutralnost Republike Srbije kao racionalno i prelazno rešenje. *Srpska politička misao*, 1, 147-188.

Gajić, A. (2023). Geopolitički položaj Srbije nakon otpočinjanja rata u Ukrajini: neutralnost i strateško odvracanje u kriznom kontekstu. *Srpska politička misao*, 2, 53-74.

Jovanović, M. (2019). Neutralnost u XXI veku: anahron ili savremen koncept? *Zbornik radova Pravnog fakulteta u Novom Sadu*, 4, 1207–1232.

Krga, B. (2017). *Strategija nacionalne bezbednosti u teoriji i praksi*. Beograd: MC „Odbrana”.

Lazić, R. (2023). *Kontrola službi bezbednosti u Srbiji*. Beograd: Fakultet za diplomatiju i bezbednost, IP „Neven”.

Lazić, R. (2022). Ekonomska bezbednost u funkciji nacionalne bezbednosti. *Politika nacionalne bezbednosti*, 1, 67-79.

Novaković, I. (2012). *Neutralnost u Evropi u 21. veku i slučaj Srbije*, Beograd: ISAK fond.

Novaković, I. (2019). *Stalna neutralnost u Evropi u posthladnoratovskom periodu*. Beograd: Institut za evropske studije.

Peta Haška konvencija o pravima i dužnostima neutralnih država i lica u slučaju rata na kopnu (Convention relative to the rights and duties of neutral powers and persons in case of war on land). 1907. Hag.

Proroković, D. (2023). Položaj Rusije u multipolarnom svetu i strateške opcije Srbije. *Srpska politička misao*, 1, 41-64.

Rezolucija Narodne skupštine Republike Srbije o zaštiti suvereniteta, teritorijalnog integriteta i ustavnog poretka Republike Srbije. (2007). Službeni glasnik RS, br. 125/07.

Simić, D. (2002). *Nauka o bezbednosti - savremeni pristup bezbednosti*. Beograd: Službeni list SRJ, Fakultet političkih nauka.

Stajić, Lj. (2021). *Osnovi sistema bezbednosti – sa osnovama istraživanja bezbednosnih pojava*. Novi Sad: Pravni fakultet.

Stajić, Lj. & Lazić, R. (2015). *Uvod u nacionalnu bezbednost*. Beograd: Akademija za nacionalnu bezbednost, JP „Službeni glasnik”.

Stojanović, S. & Šaranović, J. (2022). Vojna neutralnost i srpska strateška kultura. *Srpska politička misao*, 1, 11-40.

Strategija nacionalne bezbednosti Republike Srbije. (2009). Službeni glasnik RS, br. 88/09.

Strategija nacionalne bezbednosti Republike Srbije. (2019). Službeni glasnik RS, br. 94/09.

Strategija odbrane. (2009). Službeni glasnik RS, br. 88/09.

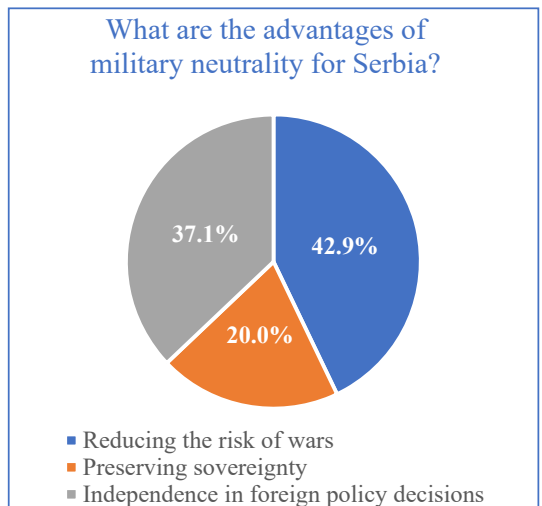
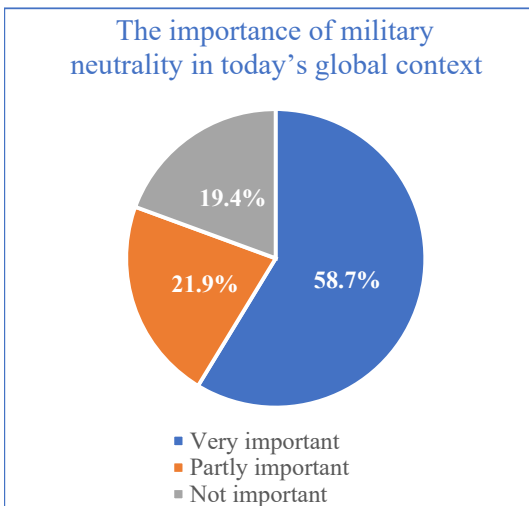
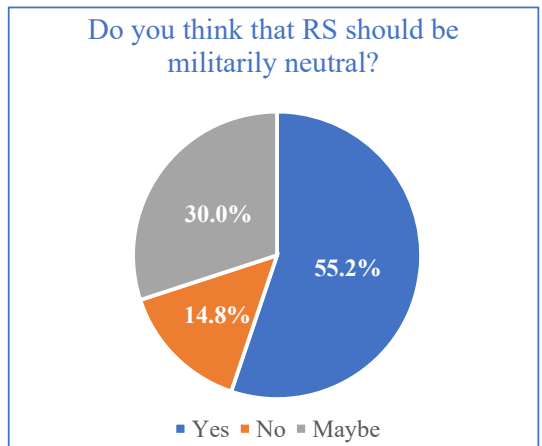
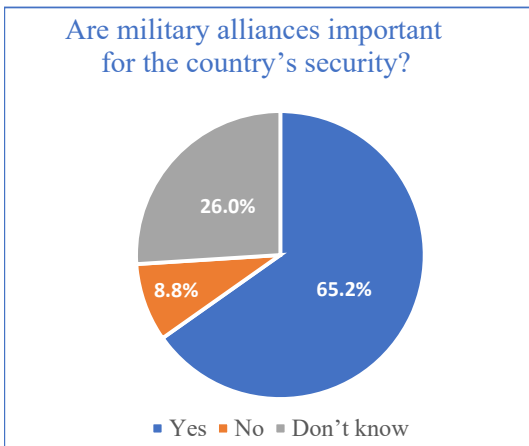
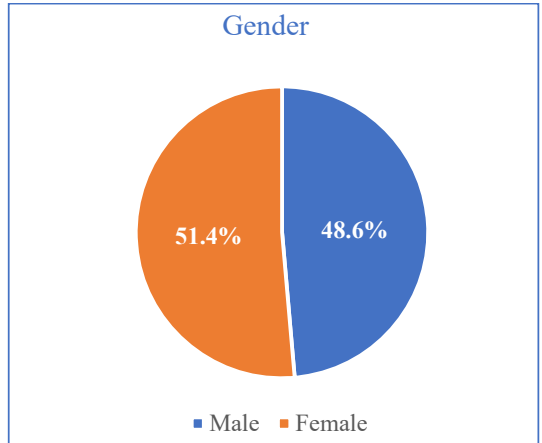
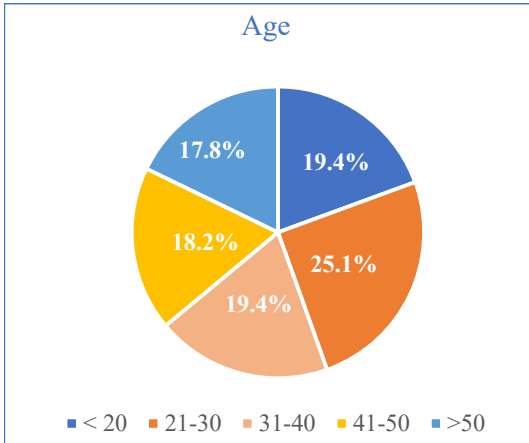
Strategija odbrane. (2019). Službeni glasnik RS, br. 94/19.

Trinaesta Haška konvencija o pravima i dužnostima neutralnih država u ratu na moru (Convention concerning the rights and duties of neutral Powers in naval war). 1907. Hag.

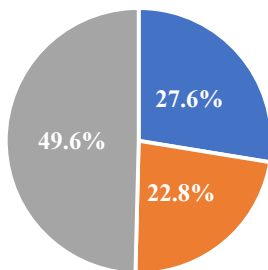
Tukidid. (1957). *Povijest peloponeskog rata, knjiga peta*. Zagreb: Matica hrvatska.

Ustav Republike Srbije. (2006). Službeni glasnik RS, br. 98/06, 115/21 i 16/22.

Appendix: Results of citizens' survey on military neutrality - N=566

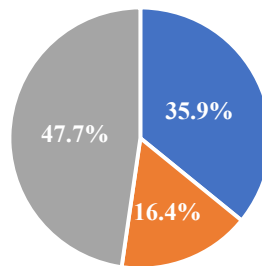


What are the disadvantages of military neutrality?



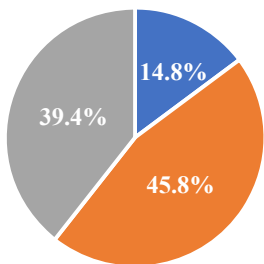
- Lack of military protection
- Limited access to military alliances and resources
- Lack of security in case of aggression

How does military neutrality affect international relations?



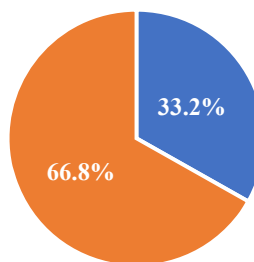
- Promotes peace and stability
- Can lead to isolation
- Facilitates diplomatic relations with all countries

Do you think that military neutrality prevents Serbia from participating in humanitarian interventions?



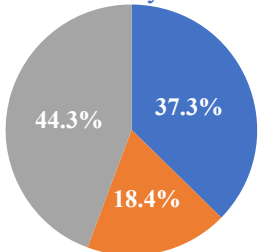
- Yes
- No
- Maybe

Would you support a change in Serbia's policy towards military neutrality?



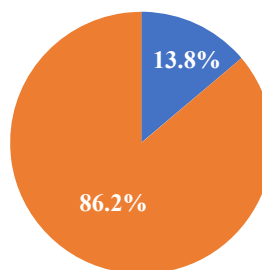
- Yes
- No

How important is it for you that Serbia remains a militarily neutral country?



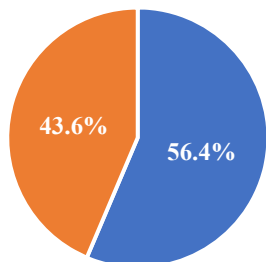
- Very important
- Not very important
- I have no opinion on that

Would you support bringing Serbia closer to military alliances such as NATO?



- Yes
- No

Do you think that military neutrality in Serbia should be the subject of citizens' referendum declaration ?



■ Yes ■ No

*Bogdana Koljević Griffith*¹
*Matthieu Grandpierron*²

FORMS OF CONTEMPORARY CONFLICTS IN THE ERA OF THE END OF NEOLIBERALISM AND BIOPOLITICS

Abstract

This interdisciplinary paper - through the interweaving of contemporary political philosophy and political theory - reflects on the issue of the conceptual framework of the forms of conflict between states and entities in the 21st century. Starting from the insight that the time of the change of eras in numerous aspects turns out to be a time of a series of wars of a local and/or regional character, it is argued that this is a logical and natural consequence of the end of neoliberalism and biopolitics. Or, more precisely, it is about the immanent consequences of political, security, economic, social and cultural neoliberalism in theory and practice, the militant character of which is its sine qua non. The analysis of the various forms of these conflicts draws attention to their biopolitical and postmodern character. The final part of the paper discusses the issue of the return of the "realist" perspective in international politics, especially in light of the transition to a multipolar world, as well as all the implications that this has for understanding contemporary forms of conflicts.

Keywords: *contemporary conflicts, neoliberalism, biopolitics, realism, multipolar world.*

INTRODUCTION: NEOLIBERALISM AS BIOPOLITICS AND A TIME OF ERA CHANGE

In political, security, economic and social terms, it is becoming increasingly clear that the time of era change is a relevant time for a series of wars of a local and regional nature (Koljevic Griffith, 2021). The most striking examples are certainly the war in Ukraine and the tragic events in Gaza, but no less important are events such as the actions of the Yemeni Houthi rebels and, in general, the fact that the modern world, in various spheres, is increasingly becoming a world of war every day. The main reasons why this type of transformation has occurred in the 21st century refer, first of all, to the fact that, from the perspective of political philosophy, the era of neoliberalism as biopolitics is ending (Foucault, 2004; Koljevic, 2010; Koljevic, 2015), which in turn - in terms of political theory and international relations - appears as the end of US hegemony, unipolarism and the concept of total domination, i.e. neo-totalitarianism. In this light, the end of the "end

¹ Institute for Political Studies, Belgrade, Serbia, bb2polfil@gmail.com

² ICES, la Roche sur Yon, France

of history" (Fukuyama 1998), or, more precisely, its rebirth and movement (Badiou, 2012; Kagan, 2009,) marked the ideological end of the dominance of the "materialist paradigm" (Badiou, 2006) and globalism via uniformitarianism on the world stage - which is designed to level all differences and erase history and collective identities. Quite naturally and logically, the time of the end of one era and the emergence of a new one is *eo ipso* a time of turbulence, but the phenomenon that the change and transition to multipolarism is theoretically and practically increasingly manifesting itself as a world of war most directly belongs to the rule of biopolitical, i.e. neoliberal discourse and politics. Moreover, it is about the final fulfillment of the concept of neoliberalism, that is, its final phase, which inevitably corresponds to phenomena such as biopolitical neo-Nazism in Ukraine – which, in parallel, is proclaimed as "heroism" (Žižek, 2022), and, in this way, neo-Nazism turns out to be the realization of the concept of neoliberalism and its last stage (Koljević Griffith, 2023).

In other words, neoliberalism via biopolitics, since the beginning of its practically absolute hegemony – and it was metaphorically and realistically marked precisely by the war against Serbia (Badiou, 2006), i.e. the "humanitarian intervention" in 1999, bypassing the UN Security Council, which demolished the foundations of international law and practically suspended and put it ad acta (a process whose dramatic consequence was the illegal and illegitimate unilateral recognition of the fake state of "Kosovo" by the majority of Western powers). This is precisely why Costamagna rightly observes that the contemporary war in Ukraine turns out to be precisely the long-term effect of NATO intervention against Serbia (Costamagna, 2023), because it is, in fact, a unique biopolitical process of general militarization that was originally initiated by the West. Ergo, almost the entire political, security, economic and social philosophy and practice of the West over the past three decades has demonstrated how the core of neoliberalism is its structurally militant character, that is, how limitless expansionism - primarily of the NATO military alliance and the EU political project - is here essentially intertwined with a utilitarian post-ethics in which all means are permitted for the purpose of total control of entire populations.

Foucault's interdisciplinary research articulates how the techniques of management and the development of microstrategies of power change historically - and how, in this regard, the Panopticon model gradually transforms theoretically and practically from the control of the individual and "discipline". Or, more precisely, this is how governance becomes governmentality as the West moves to control and regulate entire populations – and this marks a step towards biopolitics (Foucault, 2004; Koljevic, 2010; Koljevic 2015). The emphasis placed on the idea of punishment was also a key element in the work of Lakoff, who showed how this idea, the narrative of the strict father, according to him, is central to American conservative political discourse, alongside another type of discourse, i.e. the caring parent, which structures the discourse of the Democrats (Lakoff, 2002, 2008, 2009). These two narrative structures are part of neoliberal discourses and contribute to the West's effort to establish hegemonic neocolonialism. In this light, the Western "international community"

articulates the idea that any "depravity" must be punished most severely (mainly political regimes that do not follow Western models) with the argument that it is a "disease" that contaminates the rest of the world; and, in parallel, the idea that any country that does not have a political model equivalent to Western models should be "educated" like a small child.

The extent to which this research is instructive in contemporary conditions is perhaps best illustrated by the fact that, in its most essential determinations, neoliberalism via biopolitics represents for Foucault the process of fragmentation of political, security and economic sovereignty (Foucault, 2004) - and therefore the fundamental struggle in the 21st century on the world stage is precisely between sovereignty and globalism. This opposition is a key and structural element in the discourses of the BRICS countries, especially China and Russia, whether it is about the issue of territory, international law, or the militarization of outer space (Grandpierron, 2024).

At the same time, however, the *sine qua non* condition of neoliberal discourse and its practices is militarism because the conception of politics that is advocated is precisely the inversion of Clausewitz's formula, i.e. the establishment of politics as war by other means – and in fact as permanent war. Consequently, the distinction between war and peace is erased, and a state of Hobbesian *bellum omnium contra omnes* is introduced – and thus the distinction between status civilis and status naturalis is gradually leveled. In the general state of nature, which becomes a general state of permanent war of high or low intensity at practically all levels – from security, politics, economy, society to cultural and information wars – the basic emotion becomes fear, and in parallel the distinction between private (*oikos*) and public (*polis*) is erased. Or, more precisely, it is a situation of comprehensive politicization of life – in which the distinction between *bios* and *zoe*, i.e. "bare life" and "valuable life" disappears - which is why various forms of contemporary conflicts reveal their structurally biopolitical and postmodern character.

CONCEPTUAL FRAMEWORK OF CONFLICTS BETWEEN STATES AND ENTITIES IN THE 21ST CENTURY

It is undeniable that, in their external form, the forms of contemporary conflicts show similarities with numerous earlier forms of conflicts between states and entities, but even their primary categorization points to specificities that arise from their immanently biopolitical, i.e. neoliberal – and thus structurally militant character. Thus, for example, we can first talk about internal conflicts, within which we can distinguish:

- a) internal i.e. internal group conflicts that mostly take place through the politicization of society and the division into sovereignists and globalists that has replaced the traditional division into "left" and "right" (middle level) and;
- b) internal i.e. internal individual and state conflicts as conflicts within individuals and within the framework of the adoption and implementation of state strategies

in matters of articulation of one's own historical identity, political subjectivity and the direction in which an individual and/or state should develop in the future (micro and macro level).

On the other hand, external conflicts, in the most general division, refer primarily to: 1) political-ideological conflicts that arise due to cultural, religious or ideological intolerance between states, entities or certain groups (Ramsbotham et al., 2011) as well as;

2) the ambivalent relationship that has existed for centuries between humans and the development of technology, which, in the modern context, most often appears as a question of the development of artificial intelligence (AI), i.e. the question of the projection of a state in which humans, in the final analysis, turn out to be "surplus".

In the first case of external conflicts, it is a struggle between sovereigntism and globalism on the world, geopolitical level, where - in principle quantitative analysis - it is a conflict between the majority population of the world community, on the one hand, and the biopolitical, neoliberal minority of the Western world, on the other. Thus, in essence, it is mostly a global conflict against the ideology of globalism, on the basis of which a distinction is established between sovereign wars, on the one hand, and neo-colonial wars, on the other. This opposition is philosophically articulated by Amin Maalouf, who shows how globalization, enabled and supported by technological development, is directing different components of humanity increasingly towards each other, to the extent that these different components tend to become increasingly uniform (Maalouf, 2019). Yet there is a paradox: people are embracing doctrines and ideologies that glorify particularism. People are increasingly confronting each other day by day, and identity conflicts are becoming more and more violent. This is also the case with the conservative revolution that is taking place all over the world, with varying degrees of success. On the other side of the argument, we are also seeing a change. For the so-called forces of the left are demonstrating a behavior that is, to say the least, worrying: they are abandoning universalism in order to advocate for identity battles and act as spokesmen for various ethnic and social minorities. They are abandoning the project of establishing society as a whole, and are seeking to win over the majority by appealing to resentment. Their proposals are, at best, unrealistic, and at worst, totalitarian. This dimension is now extremely present in the discourses of Western liberal politicians who are quite explicitly using this as a new tool of governance and strategy to gain and maintain power.

Moreover, the most dramatic examples of modern wars that we mentioned at the beginning, i.e. the war of the Russian Federation against the NATO military alliance currently taking place on the territory of Ukraine (which is also called the total war of Russia against the West and vice versa), and Israel's war in the Gaza Strip unequivocally draw at-

tention to the fundamental difference between the forms and implications of sovereignist, i.e. defensive-patriotic, and neocolonial, i.e. offensive wars in the 21st century (in the previous classification, both belong to external conflicts). Because, the first case, namely, clearly illustrates the principled nature of the sovereignty policy pursued by the modern Russian Federation, which is based on the belief that the use of force is justified exclusively for defensive, not expansionist, purposes - which is why, among other things, throughout the entire duration of the special military operation, i.e. from the beginning until today, it has strictly ensured that force is not excessive and, above all, that it is not used against the civilian population in the territory of Ukraine, i.e. respect for international law on the battlefield as well as the so-called "Westphalian regularity" applies. This tension between the multilateral and the unilateral is reflected in the Western use of the term "international community". The justification for all coercive measures is found in the defense of the so-called 'values' of this community. In this process, the discourse of "sanctions" skillfully switches places and confuses the registers of legality and legitimacy. The use of international law through the term "sanctions" demonstrates the need to consider law as a discourse, as an instrument of legitimation, or, in other words, as an instrument of power (Anghie, 2004; Chimni, 2017; Koskenniemi, 2004). Or, in other words, this type of sovereignist, i.e. defensive-patriotic wars, is also structurally related to contemporary wars of decolonization, which, at the same time, as new forms of liberation wars, introduced a "new grammar" and a "new lexicon" into international conflicts (Badie, 2014), but also refer precisely to the restoration of political, security, economic, social and cultural sovereignty.

In parallel, the second case, i.e. the tragedy in Gaza, is an exemplary example of a biopolitical, i.e. expansive neoliberal war - as a war waged against an entire population, by all means and practically to the point of extermination, and contrary to all the rules of war, as well as international and humanitarian law and all relevant conventions. Moreover, it was precisely Israel's actions - which have practically completely abolished any connection and internal relationship between politics and ethics - as brutal and naked violence, that demonstrated what, in the final instance, the politics of "exceptionalism" means, which, with a claim to superiority, believes that it can shape the world according to its own "rules" and not according to the law (rules based order).

It was precisely this "policy of exceptionalism" that the US adopted at a historical moment when it decided not to follow Huntington's warning that America must not wage war against the Eastern Orthodox world (Huntington, 2011). Quite the contrary, America adopted and implemented the Wolfowitz doctrine, which claims exactly the opposite - and is further supported by Brzezinski's (Brzezinski, 1998) view that whoever controls Eurasia controls the entire world (Koljević Griffith, 2023). In this light, it should be emphasized that the main political and security cause of most contemporary conflicts between states and entities is precisely the NATO military alliance, i.e. its policy of expansion and expansionism practically ad infinitum. Because, in the concept of total hegemony, i.e. per

definitionem neo-totalitarianism - which biopolitical neoliberalism represents - militarism is incorporated not only into all key strategies, "mainstream" media and sources of information, but also into the entire educational system practically without exception.

When it comes to the conflict potential of the EU, it is necessary to first notice the following:

a) parallelism with the actions of the NATO military alliance and;

b) the "militaristic continuity" that has existed since the time of the NATO bombing of Serbia, through the uncritical acceptance and implementation of the US foreign policy hegemonic strategy towards the entire non-Western world through a series of examples, all the way to transparent cases of biopolitical neo-colonialism in the heart of Europe. The latter, in the contemporary context of the 21st century, is primarily visible in:

1) Bosnia and Herzegovina, primarily through the actions of the completely illegal and illegitimate so-called "high representative" who was not appointed by the UN Security Council, and through the relevant presence of foreigners in the Constitutional Court of Bosnia and Herzegovina, as well as through the constant manifestations of NATO's military power and undermining of security, as well as through the systematic violation of the Dayton Peace Agreement by Western powers, and the policy of constant external forcing of the conflict between the entities of Republika Srpska and the Federation of Bosnia and Herzegovina;

2) In the territory of Serbia, i.e. its southern province of Kosovo and Metohija, where even elections whose turnout was 3% were recognized by the West as legitimate, in a situation in which, in parallel, the policy of silent ethnic cleansing of Serbs from the entire territory of Kosovo and Metohija is tacitly affirmed.

Certainly, in the categorization of contemporary forms of conflicts, we also make a relevant distinction between armed conflicts, i.e. conventional wars and hybrid warfare (Weissmann et al., 2021), the scope of which ranges from proxy wars, a series of different information wars to rebellions and "regime change". The latter are also classified as 'gray zone' conflicts because they do not involve the direct use of force but rather the implementation of a series of microstrategies of power. Without a doubt, most conflicts in the 21st century mostly appear as an intertwining of both forms - just as is paradigmatically the case with the war in Ukraine, which represents a combination of conventional war and hybrid war, with a prominent role played primarily by Western propaganda.

On the other hand, the question arises whether the basis of contemporary conflicts is some kind of Huntingtonian clash of civilizations, but - as Dugin rightly notes - this conflict today is such that, in the era of multipolarity, as many as six civilizations are on one side - and only Western civilization on the other (Dugin, 2024). This asymmetry shows the specific nature of contemporary conflict en generale, in which the majority population advocates for open dialogue, global debate on the basis of equality and for a policy of co-

operation instead of the use of force and conflict, while, in parallel, neoliberal Western civilization is gradually transforming into a post-civilization in which the Schmittian division of the world into "friends" and "enemies" has been practically taken to the extreme. In this light, the crucial question once again becomes how to avoid Thucydides' trap (Allison, 2017; Koljević Griffith, 2022), in a situation that Mearsheimer explains as follows: liberal democracy was doomed to fail – and it failed (Mearsheimer, 2018).

In order to understand the contemporary version of the "Thucydides' Trap" in the 21st century (Koljević Griffith, 2022), it is necessary to bear in mind how this form of conflicts nevertheless goes beyond the model of classical conflicts according to Clausewitz, i.e. how conflicts between states and/or entities (interstate conflicts) turn out to be multiple and intertwined with internal, or internal conflicts in states that are on the rise – and these most often appear as a series of permanent low-intensity wars. Moreover, as Badie emphasizes, here we directly enter the field of conflict ontology in which the biopolitical basis is false humanitarianism and in which, further, the weakening of the state appears as the foundation of the peculiarity of contemporary conflicts. In this sense, Kaldor, for example, argues that the specificity of contemporary asymmetric conflicts and irregular wars is most closely linked to the processes of weakening the state as a legitimate source of norms (Kaldor 1999) and thus their core is biopolitical *par excellence*. Because, namely, 'irregular wars' refer to violent conflicts between state and non-state actors, i.e. precisely to the struggle for the management of relevant populations. Such conflicts are mostly marked by indirect and asymmetrical approaches and can include a range of manifestations – from insurgencies, through psychological and information warfare, to terrorism – and they often involve transnational criminal organizations. The fragility of the state and its constant fragmentation cause a series of political, security and social deficits that generate anomie. Failure to guarantee the individual and collective security of citizens culminates in the violation of the social contract on which the state rests. Or, more precisely, in the final instance, it is about postmodern processes of structural de(con)struction of the social contract in which - precisely as a consequence of the ideology of globalism - war ultimately appears as a general social pathology (Badie, 2014).

Thus, in the era of neoliberal biopolitics – and its end – war is no longer simply a product of conflicting interests but appears as the spread of social pathology, and the feeling of the emptiness of the state is radically present precisely in the globalized world. Consequently, the "new grammar" and "new lexicon" of contemporary forms of conflict must take into account both the social character and all the implications arising from the sphere of diversification of violence.

At the same time, conflicts between states *per se* are generated in parallel or, rather, as an integral part of the indicated processes, and they are mostly based on a) ideological, religious and/or ethnic issues or b) predominantly economic issues (Silva &

Gomes, 2016). And again, in both cases, the weakness of state institutions increases the prospects for social polarization and thus increases the risk of instability.

MULTIPOLAR WORLD AND THE RETURN OF "REALISM" IN INTERNATIONAL POLITICS – IMPLICATIONS FOR SECURITY AND MODERN CONFLICTS

The tectonic transformations brought about by the birth of a multipolar world undoubtedly open up a whole range of new perspectives and political, security, economic and social potentialities for a new era. At the heart of these efforts is, above all, the understanding of the great powers - such as the Russian Federation or the People's Republic of China, but also the countries of the "Global South" - that, precisely for the sake of world stability, it is necessary to renew the theories and practices of realism in international politics. Or, more precisely, a return to the principle of realism in international relations would, on the one hand, create a path for the eventual phased implementation of new collective security treaties, while, in parallel, on the other hand, it would mark the end of postmodernism and biopolitical neoliberalism and the restoration of sovereignty at virtually all levels.

In parallel, one of the relevant consequences of this potential transition of the world into a new era – above all for the transformation of contemporary conflicts – would be a return to a strategic security culture in which there is a clear distinction between war and peace. Also, given that all major non-Western rising powers are committed to cooperation on the basis of equality, as well as a return to international law, the methods of conflict in the post-liberal world would change significantly and would no longer include the widespread application of political and economic measures such as the international sanctions currently applied against the Russian Federation (also a biopolitical phenomenon *par excellence*). For liberal democracies, it is obvious that the international community can consist exclusively of "liberal democracies" and that, therefore, any other form of regime is illegitimate (Kuhnhardt, 2017; Pabst, 2019; Parsi, 2021; Sorensen, 2011). Thus, sanctions would allow the construction of a world composed exclusively of liberal states, and, ultimately, the distinction between "liberal democracies" and the "international community" would disappear (Buchan, 2013). Economic sanctions also allow for a response to the liberal view of war. Indeed, war is the product of the presence of the power of a violent government that the people did not elect. Thus, economic sanctions are intended to show the people (a specific population) that their government must be overthrown, because its 'bad' behavior deprives them of economic prosperity and well-being. The idea is that a dissatisfied population will rebel and move towards regime change. If, on the other hand, the population does not rebel, then it is as guilty as the government and deserves to be deprived. This is especially the case because there is a tendency to assimilate decision-makers

and their population. The population then also has to be defeated, punished (Lakoff's metaphor of the punishing father) in order to be "educated for democracy" and to cure the disease (Lakoff's metaphor of the caring parent).

Next, since this is a transition from a state of post-truth to a time of renewal of subjectivity, the majority of the world's population is, in all likelihood, committed to an end to information and culture wars and to fundamental respect for all differences and the ability of peoples and states to freely decide on their own destiny. This is a systemic theoretical and practical example of the end of hegemonic politics and the artificial division of the world into "authoritarian regimes" and self-proclaimed "democracies" – a binarism that was supposed to replace the former Aronian ideological distinction between "totalitarianism" and "democracy" (Aron, 1969).

No less important, the indicated concept of "new realism" essentially includes the end of the politicization of human rights, which was one of the main instruments of neo-imperialism and neo-colonialism of the West (Douzinas, 2007) and the so-called "humanitarianism" in whose name brutal interventions were carried out around the world with the use of incredible force. At the same time, as the end of utilitarianism, a new ethics of content could potentially be reaffirmed in various discourses and politics, with the full awareness that it can never be absolutely achieved but that what we can achieve is that the games of power are realized "with a minimum of domination" (Foucault, 2003).

Certainly, the return of sovereignty as a key political principle – based on the adoption of a *realpolitik* stance in international relations – points to a new identification of legal and political sources of authority and re-translates the question "who governs?" into new institutional frameworks. Or, in other words, it is about the re-establishment of all three dimensions of sovereignty (foundational, institutional and territorial) – and e.g. in the case of the EU it refers, first of all, to the practice of abandoning the policy of "shared sovereignty" (Bickerton et al., 2022). In this light, the sovereignist mobilization taking place in a number of European countries aims to establish true democracy as the rule of the people, i.e. popular and state self-determination against alienated national and transnational crypto-elites. For, in the broadest sense, the concept of self-establishment – which stems from a return to sovereignty and subjectivity – is once again emerging as the foundation of the political order, and it is precisely on these foundations that it is possible to build a new political and normative stabilization on the Old Continent. Consequently, Europe can use the historical moment of the change of eras to implement new social contracts and new consensuses that would rest on new security structures.

REFERENCE LIST

- Allison, G. (2017). *Destined for War*. Boston: Mariner Books.
- Anghie A (2004). *Imperialism, Sovereignty, and the Making of International Law*. Cambridge: Cambridge University Press.
- Aron, R. (1969). *Democracy and Totalitarianism*. New York: Frederick A. Praeger.
- Badie, B. (2014). Introduction: Guerres h'ier et d'aujourd'hui. In B. Badie & D. Vidal (Ed.), *Nouvelle Guerres*. (pp. 11-23). Paris: Edition La Decouverte,
- Bickerton, C., Brack, N. & Coman, R. (2022). Conflicts of sovereignty in contemporary Europe: a framework of analysis. *Comparative European Politics* 20, 257–274.
- Brzezinski, Z. (1998). *The Grand Chessboard*. New York: Basic Books.
- Buchan, R. (2013) *International Law and the Construction of the Liberal Peace*. Oxford: Hart Publishing.
- Chimni, B.S. (2017). *International Law and World Order: A Critique of Contemporary Approaches*. 2nd ed. Cambridge University Press.
- Clausewitz, K. (2010). *On War*. New York: CreateSpace Independent Publishing Platform.
- Costamagna, C. (2023). War in Ukraine as a long-term effect of NATO intervention against Yugoslavia? An overview. *Sociological Review*. LVII (2):541. 541-561.
- Douzinas, C. (2007). *Human Rights and Empire*. London: Routledge.
- Dugin, A. (2024, March 5). *Kraj ere zapadne hegemonije*. RT Balkan. Retrieved March 13, 2024, from <https://lat.rt.rs>
- Grandpierron M (2024) *Nostalgic Virility as Cause of War. How leaders of Great Powers Cope with Status Decline*. Montreal: McGill-Queens University Press.
- Huntington, S. (2011). *The Clash of Civilizations*. New York: Simon & Shuster.
- Foucault, M. (2003). *Society Must Be Defended*. New York: Picador
- Foucault M. (2004) *La Naissance de la biopolitique*. Paris: SEUIL.
- Fukuyama, F. (1998). *The End of History and The Last Man*. Washington DC: Free Press.
- Kaldor, M. (1999). *New and Old Wars: Organized Violence in a Global Era*. Stanford: SUP.
- Kagan, R. (2009). *The Return of History and The End of Dreams*. New York: Vintage.
- Koljević, B. (2010). *Biopolitika i politički subjektivitet*. Beograd: Službeni glasnik.
- Koljević, B. (2015). *Biopolitika i savremeni svet*. Beograd: Zavod za udžbenike.
- Koljević Griffith, B. (2021). *Promena epoha i Zapad na raskršću*. Beograd: CATENA MUNDI – IPS.
- Koljević Griffith, B. (2022). Posle američke „izuzetnosti“ – „Tukididova zamka“ XXI veka“. *Sociološki pregled*. Vol.56.br.3. 978-1002.

- Koljević Griffith, B. (2023). After Neoliberalism – Russia and European Values in the 21st Century. In B. Koljević Griffith (ed.) *Reinterpretation of Russia in the Twenty-First Century* (207-222.). Belgrade: IPS.
- Koskenniemi M (2004) International law and hegemony: a reconfiguration. *Cambridge Review of International Affairs* 17(2): 197–218.
- Kühnhardt L (2017) *The Global Society and Its Enemies: Liberal Order beyond the Third World War*. Cham: Springer.
- Lakoff G (2002) *Moral Politics: How Liberals and Conservatives Think*. 2nd ed. Chicago: University of Chicago Press.
- Lakoff G (2008) *The Political Mind: Why You Can't Understand 21st-Century Politics with an 18th-Century Brain*. New York: Viking.
- Lakoff G (2009) *The Political Mind: A Cognitive Scientist's Guide to Your Brain and Its Politics*; [with a New Preface]. New York: Penguin Books.
- Maalouf A (2019) *Le Naufrage des Civilisations*. Paris: Editions Grasset et Fasquelle.
- Mearsheimer, J.J. (2018) *The Great Delusion*. New Haven (NH): Yale University Press.
- Pabst A (2019) *Liberal World Order and Its Critics: Civilisational States and Cultural Commonwealths*. World politics and dialogues of civilizations series. London: Routledge.
- Parsi VE (2021) *The Wrecking of the Liberal World Order*. Cham: Palgrave Macmillan.
- Ramsbotham, O. Woodhouse, T. & Miall, H (2011). *Contemporary Conflict Resolution*. New York: Polity Press.
- Sørensen G (2006) What Kind of World Order? The International System in the New Millennium. *Cooperation and Conflict* 41(4): 343–363.
- Weissmann, M. Nilsson, N. Palmertz, B. eds. (2021). *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris.
- Žižek, S. (2022, May 11). *The Heroes of the Apocalypse*. Project-syndicate. Retrieved March 11, 2024, from <https://www.project-syndicate.org/>

Brankica Janković¹

MODERN APPROACHES TO SECURITY – FEMINIST THEORIES

Abstract

In the context of dynamic and complex conditions in intra-state and international relations, it is necessary to open space and create a supportive environment for debates and considerations of different approaches to security, in order to create the best conditions for reaching the desired state of security at all levels and in all sectors. The influence of contemporary, i.e. critical considerations and the impact on the change of traditional views on international and security in general, was particularly pronounced at the end of the Cold War, after the fall of the Berlin Wall, which traditional security theories neither predicted nor explained. A new chapter has been opened in theoretical approaches to security, in which feminist theories occupy, perhaps still insufficiently recognized and systematized, but an important place. Feminist theory introduces gender as a key concept for understanding social trends in which misogyny and patriarchy are pervasive elements of the social structure, based on unequal power relations between men and women, as a consequence of historically unequal power relations that have gained new forms of expression in modern living conditions. The perception of power, which remained dominantly male, centralized and focused on realizing the national interest as the most important for achieving the desired state of security, is key to understanding the contribution of this theoretical approach to the science of security and international relations. Feminist theories have expanded the additional field of consideration of security through a step forward in relation to the concept of human security that put the individual in focus, by adding a gender perspective - that of women, and by making contributions in scientific debates related to threats that come from the non-military sector, but also from it, and especially affect women. Gender neutrality that does not take into account women's perspectives in looking at security issues is unable to provide an answer to all the ways in which modern security challenges, risks and threats affect women's lives. The emancipatory endeavor and project that is feminism continues to develop and influence the transformation of relations in all societies, challenging the existing relations of structural inequalities and discrimination against women and other marginalized social groups, overcoming in practice the dimensions and frameworks of theoretical action through the continuous struggle for full respect of all human rights.

Keywords: *security, concept, feminism, gender, threats and risks.*

¹ Commissioner for the Protection of Equality, the Republic of Serbia

INTRODUCTION

In the research center of security studies, throughout their development within international relations, there was national security, with a state-centric approach, in which the state is the only frame of reference, in a bipolar world in which the main tools for state action are the so-called hard powers, and force politics has a key role in international relations. Almost all security threats were analyzed within the framework of a realist or liberal theoretical approach, although during this period the outlines of different theoretical and practical approaches to security issues were visible, primarily thanks to the influence of other scientific disciplines in the development and understanding of the science of international relations. The flowering of those new, critical approaches happened at the end of the last century, especially with the end of the Cold War. Everything that happened on the international stage after the fall of the Berlin Wall, which symbolically marked the end of the "bipolar world", as the situation in the "international sky" was perceived at the time, opened wide the door for modern approaches in security analysis. In the current conditions, the process of globalization, with all its advantages but also dangers, more precisely new or modified old security risks, significantly affects all aspects of politics, life and economy at the national and international level. The security of people and businesses has become as important as the security of the state itself. Safe and satisfied citizens are the key to a stable and economically fast-growing society and state. In such a changed social environment, it was necessary to take into account different theoretical considerations when it comes to security. Important debates at the world level helped to recognize the concept of Human Security as an adequate modern approach in the fight not only against challenges within nations, but also at the global level (world poverty, climate change, etc.) (Janković and Bošković, 2024: 89).

One thing is certain: the human-individual slowly becomes important for understanding the new security paradigm and slowly enters the discourse of security studies in different ways and at different levels, especially through the development of critical security studies. Security challenges, risks and threats coming from the non-military and external environment are definitely recognized as completely relevant, of course, not without criticism and obstacles inherent in the defense of the traditional approach to the value system, which, unfortunately, does not bypass the scientific community either. The feminist approach, i.e. security theory, which is the subject of this paper, certainly belongs to the body of contemporary/critical approaches to security, although we can glimpse the beginnings of feminist thinking as early as the 18th century, since the appearance of the "Declaration on the Rights of Women and Citizens" published by one of the first French feminists, Olympe de Gouges.

One of the modern concepts, widely accepted and already successfully applied in practice, is the concept of human security, which places man as an individual in the center as a reference object of security policy. This concept emphasizes that the economy,

environment, security, social conditions and the rule of law and human rights are the main attributes and conditions that provide citizens with prosperity, a sense of security and personal and collective integrity. Good socio-economic conditions, a healthy environment and respect for human rights are prerequisites for the development of stable, strong and modern democratic states. National security is also viewed through the state of the economy, the social and financial satisfaction of citizens and the overall level of political freedom and culture. For the first time, this concept was formally mentioned in 1993 in the Human Development Report, compiled by the United Nations Development Program (UNDP). This report points out that the danger of external aggression is decreasing and that military force should give way to other strategies and institutions that should preserve the socio-economic situation within the limits of stability and certainty and the political freedom of citizens in their countries and that the focus must be shifted to the security of people instead of the security of territories, as well as that special emphasis must be placed on the security of food, employment and the environment. In the next UNDP report, the one for 1994, seven dimensions of human security are defined: economic, food, health, environmental, personal, social and political security. Reflections that take into account socio-political and security events and changes over a longer period of time and the less visible potential for achievement are more than welcome and necessary in dynamic intra-state and international relations.

MODERN THOUGHTS ON SECURITY

Development is also needed in ideas and research that deal with how to ensure a dignified life for all people and security in constantly changing circumstances. The impact of more pragmatic considerations and the impact on the change of traditional views on international and security in general, as already mentioned in the introduction, was initiated especially after the fall of the Berlin Wall, with the end of the Cold War. It can be said that the dynamic development of scientific thinking and analysis in this intellectual field is, among other things, the result of the fact that the previously dominant theories did not foresee such a turn of events in a bipolar world, in which a strict bloc division reigned, and states were the main actors of the international security scene. It was necessary to take into account, or rather to set up, a different analytical framework for understanding and explaining everything that happened in that period, in which the country we previously lived in, SFRY, went through a dramatic breakdown of society and wars, the consequences of which we still feel today in the first decades of the 21st century. This, like many other "post-Cold War" events, required a new approach, a new analytical framework, and even a conceptual apparatus that was developed as an alternative direction, albeit on the margins of the dominant traditional security studies - realism and liberalism. In addition to social constructivism, which was conceived by the

works of Max Weber and Emile Durkheim, and gained a foothold in the works of Alexander Wendt and, perhaps to the general public, the best-known neorealism, "thanks" to Kenneth Waltz and his "Theory of International Politics", a very important step was taken by Ken Booth, who introduced the notion of critical security studies into the new security discourse and especially emphasized the importance of emancipation for people's security, defining "emancipation as the liberation of people from the physical and human limitations that prevent them to do what they would otherwise choose to do. War and the threat of war are some of those constraints, along with poverty, poor education, and political repression. Emancipation, not power, produces security" (Booth, 1991: 316). It seems that this approach of Booth was an inspiration to certain authors within some directions of feminist theories of security.

One of the biggest steps forward in shifting the focus from the state-centric framework and the dominant military narratives and security threats that come from "outside" was made by Barry Buzan and Ole Waever, and later by other numerous representatives of the Copenhagen School, probably the most famous among modern or critical concepts of security. The main contribution of this school is three basic ideas, first of all, the theory of securitization, the sectoral approach to security and the theory of the regional security complex. For the purposes of this paper, it is sufficient to mention that according to the theory of securitization, a key role in constructing (in)security is played by the "speech act" in the public space, which indicates, that is, identifies, the threat to security and thus actually articulates a current political problem that does not necessarily have an objective meaning. Behind this first step or act, measures are adopted, as a result of the securitization of a certain phenomenon. Of course, in order for the process of securitization to be successful, that is, for the threat to be treated seriously, which implies the undertaking of prevention and protection measures, it is necessary that the social actor carrying out the securitization has authority, i.e. legitimacy, in society, and that the threat was previously an integral part of the social fabric, created as a result of collective memory, lived experience, but often also as a consequence of the community's irrational attitudes towards certain social phenomena and identities. This theory has been exposed to numerous criticisms, which are not the subject of this paper, but at this point one can recognize what is indirectly related to the main topic of this paper - the feminist approach to security, which precisely opens debates on the topics of why, how, who and in what way determines what are the main problems of security, which is the main subject of security, who and how is protected by the measures taken. Omitting the female perspective in constructing and observing security to a significant extent can lead to significant omissions and irreparable errors in the establishment of security systems at every level.

The aforementioned development and change of the human security paradigm in the early 1990s initiated a whole series of new debates in security studies, especially in the discipline of international relations in general (Nuruzzaman, 2006: 285). The primary

focus of the argumentation was on the fundamental questions of security - for whom and how it should be achieved. Given the changes taking place in the international system, in which the forms of war and peace have changed, new events or changed forms of already known challenges have led to "great discussions" (Dunne, Hansen & Wight, 2013: 406).

Although the debate at one point of development within the realist paradigm, as the previous approaches were comprehensively called, moved from conventional warfare to non-military challenges, "this did not necessarily mean a departure from the state-centered approach to security" (Tamang, 2016: 228). In his work, Hudson (2010) quoted the then Secretary General of the United Nations (UN), Kofi Annan, who pointed out in 2004 that the biggest security threats that societies face today and will face in the coming decades go beyond aggressive wars, and they relate to poverty, infectious diseases and environmental degradation, intra-societal and intra-state violence and transnational organized crime.

It is reasonable and legitimate in the current geopolitical conditions to ask whether citizens are safe if they have a satisfactory standard, guaranteed democracy and respect for human rights through enacted legislation? Does it make communities and states really safe from crime, violence, discrimination, environmental threats? Can the state, which should be the guarantor of citizens' security, also be a source of threat to individuals? Are all citizens equally safe? This refers to whether the specificities of human needs and different perspectives that are conditioned by gender, race, religion, nationality, property status and other important determinants of social groups within the general population of the population at different levels are sufficiently taken into account.

FEMINIST THEORIES - DIFFERENT APPROACHES AND SIGNIFICANCE

In the previous part of the paper, it has been stated that the key concept that puts man as an individual in the focus of the security system and deals with issues of importance for his security, while shifting attention to human rights and human security development, is the concept of human security. Certain critics of this concept and advocates of certain schools of thought of the 21st century point out that "human" in the discourse on human security serves to qualify the discursive terrain of "security". The ways in which the interconnected categories of "human", "individual" and "vital core of all human lives" (Alkire, 2003: 23) are constructed have significant implications for the kind of "security" that can be theorized and normatively framed, but this does not mean that, in essence, they are secured. It is assumed that the individual has the innate ability to make a free choice between a number of possibilities, but also requires the fulfillment of certain minimum conditions in order to properly achieve the freedom of choice, the expansion of which is the goal of development and ensuring "human" in the concept (UNDP, 1994). The insufficient strength of the concept of human security,

but also of strategists and decision-makers, to truly ensure equality for everyone and proclaimed human rights and values, was particularly and consistently emphasized by feminist theories. Calling into question the basic premises of existing concepts of security, feminist theories call into question the state-centric and militarized definition of security and challenge the way in which both theory and practice of international relations remain highly gender-stereotyped and focused exclusively on the macro levels of interstate relations that completely ignore the gender regime and relations in which there was not enough space for women's voices.

As the UN Department of Peacekeeping Operations points out, there are three main stereotypes that prevent greater participation of women in all, including security affairs: 1) Gender-responsive analysis of conflicts is a completely separate process from the analysis of current conflicts; 2) All women have the same view of conflicts and 3) Men are soldiers, and women are victims (Janković and Bošković, 2024:91). The previous dominant approach to security, as argued in most feminist works, was based on the dominant male principle of power and the determination of the desired state of security from the point of view of dominant, thus unequal social relations that left out women's voices and their needs. The ubiquitous marginalization of women and their role and contribution in society, and reduction, exclusively to the domain of private life, favored the maintenance of patriarchal social order, which inevitably affected the state and relations in society. Patriarchal patterns influenced the situation in all spheres of social life, so they did not bypass either science or international relations.

The implementation of the concept of human security makes some significant changes in the previously established way of thinking about security:

- it indicates the shift of the reference object of "security" from the (national) state, or any limited political community or collective, to the human being, based on the understanding of people as individual, unique actors - "persons";
- it serves as an adjective that describes and enlivens a value judgment that indicates the threshold, that is, the minimum conditions for a dignified life.

However, even in this concept and the way in which, first of all, practitioners implement it, it does not mean that all people are people, the same and with equal rights and opportunities. Due to the long history of unequal power relations of marginalization of women and their exclusion from the decision-making process, especially in the field of security, then due to general gender stereotyping and division of roles, the very mention of human security associatively creates an image of men as members of the community who are the reference object. "Human rights discourse presupposes a male (white, heterosexual, able-bodied) subject – and, to the extent that such a subject is presupposed as universal, it delineates the boundaries of the 'human' and relegates others to less than human" (Marhia, 2013: 24).

"A rich feminist literature has criticized and disturbed the category of 'security' as a field of discourse and practice, emphasizing how (neo)realist conceptions of 'national' security can have disastrous political-material effects, serving paradoxically to secure certain categories of people and (re)produce (gendered and gender-based) violence" (Marhia, 2013: 20). Feminist theories did not have an easy path to the scientific or general public. One of the reasons in this case also lies in stereotypical thinking, according to which feminist theories were viewed almost exclusively from the point of view of the political demands of radical activists, while in fact the concepts talked about the core of the socio-economic and political problems of the entire community. The factual, not ideological elaboration of the issue of equality on the one hand and the security and progress of the state and society on the other, established a "focus on feminist theory, and not on social and cultural theory more broadly, because the notions of innovation and the future are interesting to examine in relation to feminism as a progressive movement" (Coleman, 2008: 86).

Feminism as a theory, and then as a political movement, strives to assess the material and value conditions of women's past and present and to propose the progress of the entire society in the future. Focusing on progression and the future allows feminist theories not to fall into the trap of pure criticism and polemics about the past. Grosz asserts that feminist theory "risks being stuck in political strategies and conceptual dilemmas that are more appropriate to the past than to the future" (Grosz, 2000: 231) while duration, as a "constant elaboration of the new" is dynamic, politics and "indeterminate response" (Coleman, 2008: 92).

Feminist theory has already developed a significant body of contemporary debate on the politics of difference, developing extensive and detailed theorizing about subject, action, and changes. "Emancipation and transformative change are fundamental to feminism, its theorizing is based on the issue of resistance" (Thomas and Davies, 2005: 713), but resistance from their discourse is positioned and expanded in terms of possibilities and offers of new visions of change and development of political and security practice. Feminist theorizing is aimed at creating knowledge dedicated to changing women's lives (ie "not only defined as knowledge of 'what' but as knowledge 'for') - the point is - to change the world, not just to study it" (Stanley, 1990: 15). A critical feminist perspective on the study of security, and especially human security, is crucial for overcoming certain "gender silences" and related violence and various victimization of almost half of the population.

Nussbaum (2000) argues that, until then, women's dormant ability to grasp the possibilities and conditions necessary for a "fully human life" stems in part from the sociocultural instrumentalization of women's bodies and work as means to the well-being and safety of others. Feminist critiques of so-called natural or depoliticized gender dichotomies within state-centric discourse delegitimize discriminatory practices and institutions as socio-historical constructions and "repoliticize" orthodox views on security

by questioning the role of the state as a provider of security (Hudson, 2005: 156). The very notion of feminism as a socio-political determinant refers to the area where the theory and practice of the transformation of unequal power relations between women and men meet. It is more than an intellectual endeavor to create knowledge (Hudson, 2005: 157). A feminist redefinition of power in terms of relationships, where the survival of one depends on the well-being of the other, improves not only the safety of women, but also of men, who are similarly threatened by conventional gendered approaches to security and by society's imposed proof of physical, economic, and combative ability, even when they themselves are deeply opposed to violence. We can say that this is an important contribution of feminist theories, from which, at the very least, the relaxation of stereotypical "musts" should result, and ultimately the general safety and freedom of decision for everyone. Another contribution of feminist postmodern theoreticians in the sphere of international relations is reflected in their fundamental "challenging of hierarchical dichotomy, such as domestic-international and dependency-sovereignty. Their work is therefore also transformative" (Hudson, 2005: 158).

The ontological and epistemological starting points of feminist theories are different, and in relation to the key reflections and recommended actions, three basic directions are distinguished - liberal, structural and post-structural. The liberal discourse of feminist theory emphasizes the equal rights of women and men within the liberal state. "Men and women are essentially equal, and gender differences are the result of gender discrimination, prejudice and stereotypes. Resistance involves reforming society/organizations to achieve gender equality and eliminate gender gaps, such as addressing barriers that prevent women from competing equally with men" (Thomas and Davies, 2005: 714-715). Structuralist and post-structuralist theories, in addition to reform, talk about much broader and more diverse forms of struggle and resistance. These theories are, one might say, much more revolutionary. "Those who promote the politics of revolution view 'woman' as a socially and politically constructed category, whose ontological basis lies in a set of experiences rooted in the material world. This shared experience of oppression unites women and acts as a catalyst for women's collective action" (Thomas and Davies, 2005: 715).

The mentioned directions of feminist theories were defined by views on inequality, oppression and problem solving. Liberal feminism focuses on removing legal barriers to women's inequality. In terms of security thinking, their goal is to shed light on the invisibility of women as participants in such systems and activities. Structuralists, with a more radical view of the problem and solution, see the source of women's oppression in patriarchy and seek a fundamental social transformation, not a "new" justice written in acts. However, even when we talk about the various struggles advocated by structural feminist theory, we must take into account that women's inequality and their oppression or exclusion from socio-political and security systems is not at the same level and of the same

type in all countries of the world. The security needs and problems of women in developed, developing and poor countries are so different that no global and unified action can be assumed. Also, "Human security as a universalistic tool of global governance must recognize differences in the degree to which the state leads or participates in the process of protecting and empowering individuals. The importance of location or context and the politics of identity for security are therefore brought into focus" (Hudson, 2005: 157).

Apart from legislative and social circumstances affecting the position of women and issues of socio-economic and political inequality, feminist theories have begun to explore the role that gender plays in areas such as war, conflict and global security (Elsh-tain, 1987; Peterson, 1992). Gender is the main analytical instrument in the feminist theory of security and international relations, but it is very complex to understand. Perhaps the best framework for its understanding was given by the feminist Ann Tickner in the extremely important work *Gender in International Relations*, in which she pointed out that the shift of the reference object from the state to the individual must take gender into account. Security risks and threats often look quite different and are prioritized according to different criteria when gender is posited as a causal variable. "Security threats must be viewed through the prism of gender glasses", that is, how security threats affect the lives of women and men (Peterson & Runyan, 1999). Tickner and other feminist authors recognize that in the new geopolitical circumstances, women are exposed to a greater number of different security risks and threats related to poverty, material deprivation, climate change, and the transnational organized crime of human trafficking. The commission of some, such as this form of crime, has been facilitated thanks to progress in the field of information and communication technologies, so today the Internet has become an important "constructive" element in the commission of crime. Feminists contribute to the debate about the need to move security risks and threats from the dominantly military sphere to the sphere of economics, ecology, politics and others, thus contributing to the expansion of the concept and definition of security, primarily through insisting that it is not enough to put an individual in the focus of security issues, but point out that, when that individual is a woman, the security paradigm acquires an additional, and often significantly different, structure. Therefore, it can be concluded that feminists provide a different structure/vision of the state and security as a condition in which men and their desirable hegemonic, "masculine" behavior are not glorified, closely linked to war and the successes that victory in war brings, which leads to further strengthening and repatriarchalization of social power relations in which women and their role in society are further devalued. From the perspective of feminists, realism is almost completely gender-neutral, and such gender neutrality must be questioned and deconstructed in the setting of a different security paradigm, by changing the approach in looking at security risks and threats. Consequently, the liberal theory is not spared from criticism either, given that especially economic and social inequalities within and

between countries affect the lives and security of women and men differently. The market conditions of liberal capitalism continuously maintain a lower valuation of women's work, primarily when it comes to unpaid housework but also in all other spheres of the economy, which leads to the maintenance of unequal economic positions in all phases of the life cycle. Such a situation reflects and reinforces the unequal position of women in all segments, especially in terms of the impossibility of making decisions at strategically important and highest decision-making levels/places.

Within numerous debates and topics, feminist theory is particularly concerned with the consequences of wars. In zones of armed struggle, women, although it doesn't seem like it, are active participants in conflicts - not only can they be fighters, and even if until then they were considered the "weaker" sex, they often become, in times of war, the new and only breadwinners for their families, active in the informal or formal sectors of the economy. In addition, women also suffer disproportionately more from deliberate and systemic sexual violence than in peace. Available data show that women are the majority of civilian victims of war, and that they are particularly disproportionately affected by rape, often as part of war booty. Yet, during and after war, women are too often excluded from activities aimed at resolving the violent conflicts that affect them so deeply (Norville, 2011: 1). The need for security of entire population groups was obviously not adequately recognized through traditional approaches, ie security theories in which national security was an absolute imperative.

Recognizing that sustainable security is not possible without the participation of women, in October 2000 the United Nations adopted Security Council Resolution 1325 - Women, Peace, Security. Women are largely excluded from formal peace processes, insufficiently represented in parliaments, governments and other decision-making bodies in countries emerging from conflicts, but also in general in legislative and executive branches of government and security systems in particular. If we want the security of the entire society and the state, through equal rights, equal access to education, work and earnings, it is necessary that women have an equal position in all spheres of political decision-making and their implementation. Social and scientific arguments and the results of the action of feminist theories certainly made a significant contribution to the understanding of the issue of gender equality and the representation of women in the security sector. From an international point of view, UN Resolution 1325 gave some national environments, even if reluctantly, a new flywheel in overcoming inequality and significant inclusion of women in defense and general security affairs, peace missions and negotiations. "Implementation of UNSC Resolution 1325 is at the very core of a much broader concept of human security, as a multidisciplinary approach, which emphasizes the protection of the individual and the prevention of factors that cause threats to his life, survival and dignity" (Janković, Banjac and Milojević, 2022: 7).

The greatest achievement of feminist ideas and thinking is precisely the placement of this topic at the international level through the work of organizations and the establishment of institutional mechanisms for gender equality at all, including national levels, through the operationalization, i.e. the adoption of national action plans for the implementation of the Resolution. In addition to the above-mentioned Resolution, the most well-known among the general public, important documents for integrating and understanding the gender perspective are also UN Resolutions 1888, 1820, 1889 and DEVAW - Declaration on the Elimination of Violence against Women, which, although not legally binding, was the first document that recognized the problem of violence against women as a systemic and structural social problem, and had a great influence on states throughout this period and changed their attitude towards the issue of gender-based violence, which resulted in establishing domestic legal frameworks for the protection of women from violence in the family and partner relationships. Due to the limited scope of the paper, we will not further deal with all aspects and scopes of the mentioned international documents or issues related to one of the biggest social problems of today - gender-based violence.

Since its adoption until today, Resolution 1325 has initiated a significant process of international conceptualization of its goals, primarily the greater inclusion of women in political and peace processes, both through negotiations and participation in UN missions in post-conflict regions, but also economic empowerment in war-ravaged areas. One of the key starting points of Resolution 1325 and its operationalization is that "the economic situation in post-conflict countries is a crucial factor in making it difficult and improving women's security" (Almagro and Ryan, 2019: 1061). Looking back at the goals and strength of Resolution 1325, the liberal direction of feminist theories suffers a certain criticism, considering that through their action, women who are outside the formal economic systems, remain "invisible". In this segment, the theory and strength of structural feminism is much clearer; it indicates that "parliaments cannot do much to improve women's security because these are structural factors, including structural adjustment policies, and neoliberalism is responsible for many insecurities that affect women workers in the informal sector" (Almagro and Ryan, 2019: 1061).

CONCLUSION

In modern scientific approaches to international security, feminist theories have become indispensable for consideration and application in the segments of not only law, politics, culture, philosophy and economy, but also security. Their importance today is not negligible, and their influence on considerations about security in general and the essence of threats is important for understanding the broader, primarily sociological context of the threat of societies and civilization. Feminist reflections have a very high

potential for further transformation and elaboration of numerous topics of importance for security at all levels and in all sectors. Numerous topics were opened and are being opened, such as the necessity and significance of women's participation in decision-making processes important for people's lives, then the responsibility of states to protect women from violence, the relationship between women and peace, issues of the use of language in the security discourse and its instrumentalization in attempts to exclude women from the mainstream of society.

Feminist theory derives from an ontology of social relations, especially gender relations, which begins at the level of the individual who is embedded in a hierarchical social, political and economic structure (Tickner, 2004: 44). If an entire group, which makes up at least half of the world's population, is unequal in all important segments of life, such a situation cannot, in the end, bring stability and progress neither to society nor to countries.

Since the adoption of Resolution 1325 and its practical application in numerous countries of the world, there is still a huge quantitative and qualitative inequality, to the detriment of women who occupy high political and security positions. Although there are many examples of women's participation in community peace building, their participation in peace processes is still limited (O'Reilly and Súilleabháin, 2013). This is not a problem of the concept of Resolution 1325, this is precisely the security problem of those who advocate peace negotiations, but do not see the wider picture of the position of women in war and their political and socio-economic opportunities in peace, including negotiations. "Today, women hold 10 of the 74 senior mediation positions in the UN (14%), which is not much, on the contrary, but still significantly more than in comparison to the 1990s or early 2000s" (O'Reilly and Súilleabháin, 2013: 4).

Feminist theories were created and propagated to the greatest extent by women, scientists and activists, but the importance of this school of thought today is evidenced by the fact that "more and more men are working as researchers in this field" (Gasztold, 2017: 180). There are significant scientific and social reasons to consider these theories not only as a collection of knowledge, but as a multidimensional and multidisciplinary approach to a deeper and more purposeful understanding and achievement of security and productive political relations. In addition to human and societal security, the feminist movement also brings significant shifts from traditional categories of security in moments when societies boil over from growing economic, social and "pressures of gender inequality, race, nationality and class, in global politics" (Sjoberg, 2016:16).

"The personal is political, it means that the personal is international" (Enloe, 2010), is one of the main determinants of feminist theory in considering the place of these theories in international relations; it deals with the way of women's exit from the private sphere through the connection with the international so that, until recently, marginal topics, reserved only for women, become relevant enough for consideration in a wider social and scientific discourse. As a reminder, the extremely difficult security

problems of women were neglected, without taking the category of gender into account, such as domestic violence, rape, denial of the right to abortion, childbirth in difficult conditions and many others. Building on this angle of looking at personal and collective security, feminist theories presented on the platform of the national and international public "previously invisible or insufficiently studied topics in the theorization of international relations - the connection between the center of global politics and the margins, the connection between political economy, personal security and international security, and the connection between gender, race and class in security" (Yuval-Davis, 1997). Thus, the coverage of the scientific impact of feminist theories in terms of national and international security and politics is intersectoral and multifaceted, not only for the issue of gender, but equality, human rights and social development in general.

REFERENCE LIST

- Ahmed, S. (1998). *Differences That Matter: Feminist Theory and Postmodernism*. Cambridge: Cambridge University Press.
- Alkire, S. (2003) A conceptual framework for human security. *CRISE Working Paper 2*. Oxford: Centre for Research on inequality, Human Security and Ethnicity.
- Almagro, M.M. & Ryan, C. (2019). Subverting economic empowerment: Towards a postcolonial-feminist framework on gender (in) securities in post-war settings. *European Journal of international Relations*, Vol. 25(4) 1059–1079.
- Booth, K. (1991). Security and Emancipation. *Review of International Studies*, Vol. 17 (4)313-326.
- Coleman, R. (2008). 'Things That Stay' Feminist theory, duration and the future. *Time & Society* Vol. 17 No. 1 (2008), pp. 85–102.
- Elshtain, J. (1987). *Women and War*. Brighton: Harvester.
- Enloe, C. (2010). *Nimo's War, Emma's War: Making Feminist Sense of the Iraq War*. Berkeley, CA: University of California Press.
- Enloe, C. (1993). *The Morning After: Sexual politics at the End of the Cold War*. Berkeley, CA: University of California Press.
- Gasztold, A. (2017). *A feminist approach to security studies*. *Przegląd Polityczny*, PP 3' 17 179-189.
- Grosz, E. (2000) 'Deleuze's Bergson: Duration, the Virtual and a Politics of the Future', in C. Colebrook and i. Buchanan (eds) *Deleuze and Feminist Theory*, pp. 214–34. Edinburgh: Edinburgh University Press.
- Hudson, H. (2005). 'Doing' Security As Though Humans Matter: A Feminist Perspective on Gender and the Politics of Human Security. *Security Dialogue* vol. 36, no. 2, 155-174.

Janković, B., & Bošković, M. (2024). Značaj primene Rezolucije SB UN 1325 u ostvarivanju stanja humane bezbednosti. *Srpska politička misao*, No 2/2024. Vol. 84, pp. 87-103.

Janković, B., Banjac, B. & Milojević, N. (2022). *Izveštaj o monitoring sprovođenja NAPA za primenu Rezolucije 1325 Saveta Bezbednosti UN – Žene, mir, bezbednost u Republici Srbiji (2017-2020)*. Poverenik za zaštitu ravnopravnost Republike Srbije.

Marhia, N. (2013). Some Humans Are More Human than Others: Troubling the 'human' in human security from a critical feminist perspective. *Security Dialogue* 44(1) 19–35.

Norville, V. (2011). *The Role of Women in Global Security*. US institute of Peace.

Nuruzzaman, M. (2006). Paradigms in Conflict. The Contested Claims of Human Security, Critical Theory and Feminism. *Journal of the Nordic international Studies Association*, Vol. 41(3): 285–303.

Nussbaum, MC (2000) *Women and Human Development: The Capabilities Approach*. Cambridge & New York: Cambridge University Press.

O'Reilly, M. & Súilleabháin, O. A. (2013). *Women in Conflict Mediation: Why It Matters*. International Peace institute.

Peterson, V. S. (1992). 'Security and Sovereign States: What is at Stake in Taking Feminism Seriously?' in V. Spike Peterson, ed., *Gendered States: Feminist (Re)Visions of international Relations Theory*. Boulder, CO: Lynne Rienner (31–64).

Sjoberg, L. (2016). What, and Where, is Feminist Security Studies? *Journal of Regional Security* (2016), 11:2, 143–161.

Stanley, L. (1990) *Feminist Praxis*. London: Routledge.

Thomas, R., and Davies, A. (2005). What Have the Feminists Done for Us? *Feminist Theory and Organizational Resistance. Organization*. Volume 12(5): 711–740, iSSN 1350–5084

Tickner, J.A. (2004). Feminist responses to international security studies. *Peace Review: A Journal of Social Justice*, 16(1), 43–48.

Tickner, J.A. (1992). *Gender and international Relations*. New York: Columbia University Press.

United Nations Development Programme (UNDP) (1994) Human Development Report 1994: New Dimensions of Human Security. New York and Oxford: Oxford University Press.

Yuval-Davis, N. (1997). *Gender and Nation*. London: Sage.

Milica Bošković¹

Mina Suknović²

SOCIETAL SECURITY AT GLOBALIZATION – LANGUAGE AS TOOL AND OBJECT OF SECURITIZATION

Abstract

In the most straightforward terms, securitization entails bringing into existence a real or imagined threat through a verbal act. The theoretical concept of securitization involves three essential components: the securitizing actor, who performs a verbal action or speech act; the referent object, which is perceived as under threat; and the audience, which must be convinced that certain (often urgent or extreme) measures are necessary to protect the securitized object, thus ensuring the safety of society, the state, and the individual. The illocutionary aspect of the speech act reveals the intention of the securitizing actor, who seeks to assert power (both personal and rhetorical) and influence the audience. Depending on the chosen object of securitization and the actor's ultimate aim, the process can sometimes be no more than rhetorical manipulation, strengthened by subjectivity and social status, rather than the presentation of objective analyses and evidence.

Keywords: *Securitization, Language, Speech Act, Objectivity*

INTRODUCTION

Following World War II, and particularly during the period marked by tension between two major military-political alliances, alongside prevailing national security strategies and the dominance of military concepts, the 1970s and 1980s saw the emergence of alternative scholarly perspectives on security. These new security concepts primarily arose from academic communities in Western Europe and, to some extent, the United States. While state-centric security concepts remained predominant, alternative modes of thinking were proposed, prioritizing individual and societal dimensions of security (Bilgrin, 2003:203). Advocates of peace organizations, such as Third World Security, strongly emphasized that state-oriented approaches to security could no longer encompass and address the growing challenges. Critics of prevailing concepts pointed out that previous security policy formulation and management had been based solely on the existence of the "Iron Curtain", and beyond this unquestionable circumstance, challenges emerged that were not strictly national, military, or state-oriented. Advocates

¹ Faculty of Diplomacy and Security, Belgrade, Serbia, milica.boskovic@fdb.edu.rs

² Faculty of Diplomacy and Security, Belgrade, Serbia

of Third World Security were concerned about the neglect of longitudinal security processes – developmental processes that maintain the security of individuals and social groups (Bilgrin, 2003:203). Among the first to embrace this new concept of thinking and policy implementation were the so-called non-aligned countries, whose neutral position between the military-political East and West allowed decision-makers to recognize internal risks. However, the dark side of this concept was the abuse of power and the bypassing of democratic processes, justified by the need to protect the population.

In the post-Cold War era, the scholarly debate on security continued at an even greater and more diverse pace, with the concept of Human Security standing out. All intra-state and intra-societal challenges, partially invisible during the era of propaganda of hostile ideologies and armies beyond state borders, now came to the forefront. Emerging challenges manifested in: (a) growing disparities in economic capabilities within and between states; (b) increasing socioeconomic difficulties faced by marginalized people in the globalized world economy; (c) depletion of non-renewable energy resources; (d) growing negative sentiments towards foreigners and violence as a reaction to migratory pressures from developing countries; and (e) intra-state conflicts, class differences, and interpretations of human rights. "Regardless of the contemporaneity of approaches, the fulfillment of the basic functions of the state is mutually conditioned and connected – security cannot be achieved without socio-economic stability and equality in society, equal application of the law for all individuals, and cooperative relations with other states. On the other hand, guaranteed rights to life and work and free will cannot be sustained without the protective function of the state" (Bošković, 2010:26). The concept of Human Security as a reference object for protection places the community and the individual, and as the pillars of security, the areas of economy, environment, human rights, and defense. Representatives of the so-called Copenhagen school, foremost among them Buzan and Wæver, not only developed the concept of Human Security but also that of Societal Security, as well as "securitization". While Societal Security places the protection of the community – its collective identity and welfare – at the core of consideration and activity, securitization seems to have erased many of the prosperous and humane ideas of the Copenhagen school. Buzan himself emphasized "that the Copenhagen School moves away from a security perspective based on the objectivity or subjectivity of threat perception. Security is understood as a speech act capable of influencing decision-making processes on security issues" (Buzan et al, 1998:26).

SECURITIZATION AND THE POWER OF UTTERANCE

Simply put, when we engage in securitization, we bring an existing or non-existing danger to life through a speech act. The theoretical concept of securitization implies the existence of a securitizer – the one who performs the speech act – then the

referent object that is threatened, and the public, which needs to be convinced that certain (often urgent or extreme) measures need to be taken to ensure the security of the object of securitization, and thus society, the state, and the individual as a whole. Depending solely on the illocutionary force of the speech act, rather than the reaction of the audience, the Copenhagen School characterized the theory of securitization (TS) as self-referential (dos Santos, 2018:228). The illocutionary aspect of the speech act speaks to the intention of the speaker – the securitizer – to express power (their own) or the spoken word and leave an impression on the message recipients. Following Austin's division of speech acts and seeking meaning in the spoken word – the locutionary approach would be much more credible for an honest approach and description of the threatened referent object. This is particularly evident when there is a risk that the public may not interpret the illocutionary verbalization of danger in the desired manner. "Given that we know (in Austin's sense) the meaning of an utterance, there may still be a further question as to how what was said was meant by the speaker, or as to how the words spoken were used, or as to how the utterance was to be taken or ought to have been taken. In order to know the illocutionary force of the utterance, we must know the answer to such questions." (Nuccetelli and Seay, 2008:338).

Buzan and Wæver developed the theory of securitization, aiming to provide an explanation of security that could focus not on material capabilities or subjective aspects but on discourses or speech acts. According to them, security is "quality actors inject into issues by securitizing them, which means to stage them on the political arena" (dos Santos, 2018:230). Securitization was first theorized by Wæver, in his 1989 work, where, using Austin's philosophy of language and speech acts (1962), he introduced a discursive approach to security that differed from the objective and subjective perspectives used until then. In the theory of speech acts, when a state representative uses the term "security", he or she shifts the issue in question into a particular arena, seeking a special right to use necessary means to block the development of the threat (Wæver 1989: 5-6); similarly, for Buzan, "security does not fall into the same dimension as everyday politics" (Buzan et al, 1998: 24-5) – to securitize a problem means to place it in the domain where urgent steps must be taken to ensure the survival of the referent object (dos Santos, 2018:232). Wæver even goes as far as to identify the so-called "facilitating conditions" that enable the transformation of a speech act into a security act – by using the grammar of security; in fact, it is precisely through the illocutionary speech act, combined with the use or misuse of the "social capital" of the securitization actor, that any object, phenomenon, or person can be securitized, especially if there are "favorable" historical, traditional, and cultural predispositions, directing public attention and preparing it for measures that must be taken achieves the full goal. The illocutionary act constitutes a meaningful statement associated with performative power. The perlocutionary act is a meaningful statement combined with a certain power that leads to

an unconventional effect. TS uses exclusively the illocutionary act (dos Santos, 2018:232). The public are "those the securitizing act attempts to convince to accept exceptional procedures, because of the specific security nature of some issue" (Buzan et al. 1998: 41). Balzacq emphasizes that the public plays an important role in legitimizing the act of securitization. Securitization is aimed at the audience and is better understood as a "strategic (pragmatic) practice that occurs within, and as part of, a configuration of circumstances, including the context, the psycho-cultural disposition of the audience, and the power that both speaker and listener bring to the interaction" (Balzacq, 2005: 172). By promoting the concept of Human Security, and later derived from it, Societal Security, Buzan sought to establish the primacy of comprehensive security on the national and international stage. In addition to the state, he identified at least three other spheres to which the concept of the referent object could be applied: the individual, the region, and the international system. He also presented society, the economy, and the environment as elements of security discourse, allowing the referent object of securitization to be anything whose survival could be threatened. Through the speech act, anything, be it material or immaterial heritage (and we can then assume – even authorities), can be securitized, and the public prepared for the necessary actions to eliminate threats.

"Throughout history, political leaders have sought to strengthen their position and justify decision-making through persuasive speeches aiming at establishing approval among an audience. According to western linguistic, sociopsychological and behavioral tradition, language and politics are two disciplines that are intimately and fundamentally linked" (Kjær, 2020:1). In discussions concerning security, politicians use linguistic strategies and discursive approaches to legitimize extraordinary actions. Consequently, a political issue evolves into a security problem through discursive politics (Balzacq, 2011). It can be said that the use of securitization as one of the goals has legitimization of security measures which are to be taken. Legitimization is the primary goal that decision-makers seek to achieve, and securitization and its narrative enable them to do so. Since language constitutes the social world, this fact includes security and its characteristics (Köhler et al, 2019:42). The process of legitimation takes place through argumentation in the form of reasoning and through presented explanations seeking approval of social actions, ideas, thoughts, and declarations (Kjær, 2020:2). Through the illocutionary speech act and the power of position, securitization actors do not wait for public approval but simultaneously create it themselves. Thus, securitization can be viewed both as a theory and as a methodology (Kjær, 2020:10).

The methodological approach helps actors choose words and phrases, tone of voice, but also non-verbal behavior, with which to successfully securitize but also create necessary legitimacy. The concept of securitization bases its methodology on the idea of speech acts and offers a methodological procedure that an analyst can use to observe and thus evaluate whether speech acts meet the criteria for securitization (Kjær, 2020:10).

Understanding the significance and necessity of "correct" securitization methodology is aided by Wæver's view that "successful securitization tends to involve the articulation of threat, only from a specific place, an institutional voice, by elites" (Wæver, 1995:57). Public acceptance of securitization and achieving legitimacy depend on the form of speech acts and the position of the securitization actor. These components of speech acts operate under what is called internal and external facilitating conditions (Buzan et. al, 1998:32). Since the public is not necessarily always (on the contrary) fully informed about all phenomena, occurrences, and events presented to them, collective attitudes and potential support often rely on the discourses of state officials because they are "places of constitutional legitimacy and therefore must have a 'good reason' to declare an issue a threat to the survival of the state" (Kjær, 2020:16). The socio-political position of securitization actors, especially if they originate from the security sector, places them in a potentially successful position as promoters of securitization because, in this case, "speech acts are conceived as forms of representation that not only reflect a tendency or view of external reality but also have a performative effect" (McDonald, 2013:72).

Three necessary circumstances, some of them facilitating for actors, for successful securitization and gaining legitimacy are: (1) the demand internal to the speech act of following the grammatical plot of designating an existential threat and arguing for urgent untypical action (Buzan et. al, 1998:32), (2) the social conditions regarding the position of authority for the securitizing actor (3) the features of the alleged threats. Devoid of arbitrariness and self-determination, securitization can be the process of constructing a shared understanding of what should be considered a threat and what should be collectively responded to. Instead, by chosen and projected speech acts, security becomes a self-referential practice – it becomes something by designating it as a security issue (Baysla, 2020:3). Therefore, it is not surprising that Behm's statement that securitization raises levels of state intervention in addressing issues in a way that portrays, emphasizes, and enhances the power of the state and its control over its citizens (Behm, 2020:1) stands out as a danger of unjustified securitization, as a feature of abuse of power, is the spread of fear and panic. Depending on the choice of the object of securitization and the ultimate goal of the actor, sometimes it is just rhetorical manipulation, enhanced by subjectivity and social position, instead of presenting objective analyses and evidence. "Issues that may be either causes or consequences of anxiety within the community are presented as existential threats requiring military or quasi-military responses. The language used to exaggerate risks is always full of hyperbole and specific rhetorics, and the proposed solutions are usually formulated in the language of urgency" (Behm, 2020:3).

LANGUAGE AS AN OBJECT OF SECURITIZATION

Societal security, stemming from Human security, regards the community and its characteristics as the referent object. Societal security relates to a society's ability to preserve its essential attributes amid changing circumstances and despite potential or actual threats (Hough, 2004:106). The community's awareness of its own security or vulnerability may differ from the perception held by decision-makers at the national level. Viver emphasizes that the community is the referent object of societal security and that its preservation differs from that of the state, even noting that external threats to the state may not necessarily mean a threat to society (Wæver et al, 1993:46). Language, written and unwritten customs, material and spiritual values, are some of the characteristics of every society/nation and also possible objects of endangerment, hence securitization. Language and alphabet represent essential and prominent features of every nation and culture (Boranijašević, 2021:230).

Globalization and its inevitable aspect of technological advancements and interconnectedness have brought positive impacts, such as faster exchange of ideas, linking scientists, knowledge about values, and the level of human rights worldwide; however, "there is also a tendency to preserve local cultures in the growing global world, encouraging multiculturalism and coexistence of diverse cultural and linguistic substrates" (Gravranović, 2003:93). It seems that language, verbal/written, symbolic and virtual, is most affected by globalization and uncontrolled exchange and establishment of both existing and newly created trends. Words, besides their referential, lexical, and denotative meanings listed in dictionaries, also have derived, emotional, specific, and socio-culturally conditioned meanings (Novosel 2007: 330). Social networks and applications, which have become an almost inseparable aspect of everyday life and work activities, as well as hobbies, often emit specific linguistic expressions (increasingly shaped in the form of symbols and images/emojis), which begin to find their place even in lively, and even official discourse. "Foreign words such as 'mobile phone', 'internet', 'surfing the internet' are used daily, often without the knowledge that these are actually words of foreign origin. This is a process during which foreign, English, words gradually enter everyday speech of adults, and indirectly even children of primary school age. Social networks have further facilitated the penetration of words of English origin into everyday speech" (Miljković, 2021:104). It is unquestionable that language, with its grammar, vocabulary, direct and indirect meanings it emits, is not a complete and unchangeable entity. Language is a characteristic of society, but also of time, complex social and political circumstances. "Languages and their alphabets have undergone certain modifications throughout history. Standard literary language in one country, or in several countries (an example being German, which is the official language in Germany, Austria, and part of Switzerland), represents a common characteristic of different dialects that may appear in one language" (Boranijašević, 2021:231). We witness that the Serbian language, in relation to all the

mentioned influences and events, has introduced many foreign words into everyday expressions for years, primarily from the English language. The adoption of foreign words is facilitated through the school system and learning of foreign languages, the use of internet applications, but also the undeniable need of young people to develop their way of communicating and conveying thoughts, messages, and emotions.

Already at this point, many would consider that language, which is a means of securitization, should now become its object. Perhaps even less writers and professors, and more decision-makers, would use speech acts to show how language and writing are threatened, by using anglicisms, Latin script, unofficial speech abundant in new, even invented terms, i.e. neologisms. If so, then the term "sekurizacija" should be removed and replaced with an appropriate expression from the Serbian language. But what would that expression be? Some authors use the word "obezbeđivanje," which is not adequate to the essence of the matter. The point is that the term, in this case, an Anglicism, carries extensive theoretical and empirical considerations and definitions, which have spawned and made this term unified. Similarly, with terms that are deeply used in practical and academic contexts – "menadžment," "SWOT analiza," "sajber prostor". At this point, we can pose an important question, relevant to both society and science – how visible and understandable will authors be to the academic community outside our borders if they exclusively use Cyrillic or persistently attempt to replace anglicisms inadequately with expressions native to their language or if they do not publish papers in English or another widely spread language? In the era of global connectivity, is it possible to "rigidly" confine ourselves to our own linguistic and cultural frameworks? Jenkins believes that even if the form used as an anglicism differs from the original, it should not be rejected as incorrect (Miljković, 2021:105). "Another reason for the increasing appearance of anglicisms is the moment where authors are unsure whether to write in their native language or English. If authors wrote in English, not in their native language, their work would be accessible to a global audience" (Zečević 2013: 23). Undoubtedly, as social beings, we should preserve distinctive characteristics, after all, written and unwritten norms and values are part of the socialization of every individual, but a crude rejection of every adaptation that has positive impacts on supranational communication, understanding, and exchange of knowledge, perhaps goes against the interest of technological and, as seen in the example, scientific progress. Moreover, while trying to "monitor" and protect children while they are on social networks, we do not translate expressions for them, but we try to warn them with the language of applications.

CONCLUSION

Despite certain advantages and popularity gained in recent decades, the theory of securitization has several limitations, but also possibilities of misuse. One of the most

criticized aspects, which is also a key element of securitization, is the focus on speech acts. According to McDonald, the theory overemphasizes speech acts while neglecting other processes or means of communication, such as images and other visual representations like videos, which also play a significant role in the process of securitization (McDonald, 2013), especially today, when social networks are often the first means of advertising and conveying messages even by political officials. "Security policy today is not only constructed with their linguistic legitimation in mind; they are now increasingly decided in relation to acceptable rhetoric of image." (Behm, 2020:10). In addition to images and other visual representations, scholars of the Paris school also emphasize the role of security professionals' practice – the authority and institutionalization of securitization actors, the routinization and repetition of messages achieve a greater effect on the audience than the magical power of speech acts. Then, according to Balzacq (Balzacq, 2011), the role of the public is insufficiently defined, due to Viver's reliance on the theory of language and who sends the messages. To persuade the audience, the speaker must adapt their language to the experience of the audience (Bigo, 2007). The excessive emphasis on speech acts and insufficient analysis of the audience(s) within the theory of securitization stem from the Copenhagen school scholars' tendency to see securitization as a universal phenomenon (Behm, 2020), without considering the existence of possibilities and powers for critical reasoning. We can say that the defense against unjustified and manipulative securitization, as well as the real protection of values or objects that are genuinely threatened, lies in the power of education, analysis of facts and the world around us, and freedom of speech and criticism.

REFERENCES

- Behm, A. (2020). *Securitisation – Turning Problems into Threats*. The Australia Institute, 1-14.
- Austin, J. L. (1962). *How to Do Things with Words*. Oxford: Oxford University Press.
- Balzacq, T. (2011). *Securitization Theory: how Security Problems Emerge and Dissolve*. Routledge.
- Balzacq, T. (2005). The three faces of securitisation: political agency, audience and context. *European Journal of international Relations* 11 (2): 171-201.
- Baysal, B. (2020). 20 Years of Securitization. *Uluslararası İlişkiler / International Relations* , 2020, Vol. 17, No. 67 (2020), pp. 3-20 (“SEK 3”)
- Bigo, D. (2007). Political Sociology and the Problem of the international. *Millennium*, 35(3), 725-739. <https://doi.org/10.1177/03058298070350030401>
- Bilgin, P. (2003). Individual and Societal Dimensions of Security. *International Studies Review*, Vol. 5, No. 2 , pp. 203-222.
- Boranijašević, M. (2021). The Serbian language and Cyrillic in everyday life

and the media. *Social Horizons*, Vol. 1 / No. 2, 230-240.

Bošković, M. (2010). *Izazovi industrijskog društva: nove tehnologije i ekološka bezbednost*. Fakultet bezbednosti, Beograd.

Buzan, B. & Wæver, O. & De Wilde, J. (1998). *Security: A New Framework for Analysis*. London: Lynne Reinner Publishers.

Dos Santos, M.C. (2018). Identity and Discourse in Securitisation Theory. *Contexto internacional* vol. 40(2) May/Aug 2018, <http://dx.doi.org/10.1590/S0102-8529.2018400200003>

Gavranović, V., Prodanović, M. (2023). Kulture u prevodu: ka očuvanju autentičnog izraza u procesu književnog prevođenja. *Baština*, 93 -103 DOI: <https://doi.org/10.5937/bastina33-36671>

Hough, P. (2004). *Understanding Global Security*. New York: Routledge.

Kjær, S.A.E. (2020). *Securitization and the Power of Language*. Faculty of Culture and Society Department of Global Political Studies Peace and Conflict Studies Bachelor Dissertation

Köhler, J., et al. (2019). An agenda for sustainability transitions research: State of the art and future directions. *Environmental innovation and Societal Transitions* 31(1), DOI:10.1016/j.eist.2019.01.004

McDonald, M. (2013). Constructivisms in Williams, P (ed.) *Security Studies: An introduction*. 2. edition. Routledge.

Miljković, M. D. (2021). Razlike u upotrebi anglicizama u svakodnevnom govoru kod dece osnovnoškolskog uzrasta u odnosu na sociodemografske varijable. *Baština*, 103-113 sv. 54, 2021

Novosel, B. (2007). *(Ne)mogućnost analize elemenata kulture. Jezici i kulture u kontaktu*. Ur. dr Igor Lakić i dr Natasa Kostić. Podgorica: Institut za strane jezike, 326-333.

Nuccetelli, S., & Seay, G. (2008). *Philosophy of Language: The Central Topics*. Rowman & Littlefield.

Wæver, O. (2011). *Politics, Security, Theory. Security Dialogue*. Special issue on The Politics of Securitization.

Wæver, O. (1989). Security, the speech act: analyzing the politics of a word. in: *Research Training Seminar*. Jerusalem/Tel Aviv, 25-26 June 1989. Copenhagen: Centre of Peace and Conflict Research.

Wæver, O., Buzan, B., Kelstrup, M. and Lemaitre, P. (1993). *Identity, Migration and the New Security Agenda in Europe*. London: Pinter.

Zečević, S. (2003). „Prošlost, sadašnjost i budućnost engleskog jezika kao globalnog jezika savremenog društva“. <file:///C:/Users/Home/Desktop/Bastina%20-%20Leposavic/Bastina-broj-35.pdf>.

Katarina Šmakić¹
Divna Vuksanović²

MEDIA AND NON-MILITARY THREATS IN HYBRID WARFARE: CAPTOLOGICAL TOOLS – PROBLEM-BASED APPROACH

Abstract

The paper explores part of the complex landscape of non-military threats within hybrid wars, using a captological research framework. The study deals with the use of captological tools for the purpose of manipulating information (via modern media) with the use of mimicry psychological operations, and technological means of induced subversion as unconventional means of warfare. The analysis aims to point out the possible non-military threats of misuse of these tools, and to advance the understanding of new technologies applied so that they pose a security challenge, providing insights that may be relevant to effective defense strategies in the age of hybrid warfare.

Keywords: *hybrid warfare, captological tools, information manipulation, psychological operations, technological subversion.*

Can future wars be anticipated based on current strategies and warfare techniques? From today's point of view, the military use of force is still an integral part of wars, supplemented by many other forms of warfare; for example, acting through known forms of (ideological, religious, media) propaganda, as well as the use of new discoveries in the field of psychology, neurology, robotics and communication technologies. Contemporary warfare is becoming more and more hybrid, thus blurring the boundaries between warfare and peacetime existence, and new possibilities of warfare based on non-military strategies are being explored.

Analyzing, in a historical interpretive context, states that constantly waged wars, and conflicts in class-divided societies, we will notice that such clashes were often resolved by adopting radical measures, that is, by armed struggle between warring parties or classes (this means revolutions). Given that no government could use exclusively radical measures, supplementary means of warfare were also used, taken from the domain of religion and customs (for example, the maintenance of cults of dead rulers and heroes served, in a certain sense, as propaganda intended for both the own population and the external enemy, etc.).

¹ Faculty of Diplomacy and Security, Belgrade, Serbia, katarinasmakic@gmail.com

² Faculty of Dramatic Arts, Belgrade, Serbia

It is known that the word "propaganda" comes from the Latin language; the noun is derived from the verb "propagare", which means "to spread", "to extend" or "to promote" (someone or something). The term was originally used in the context of spreading religious truths and teachings, especially in the Catholic Church, denoting efforts to bring religious truths to unbelievers. During the 17th and 18th centuries, the word "propaganda" was widely used in the context of promoting religious ideas and teachings; in the 19th century, the term began to be used in a political context, especially during the French Revolution. The term "propaganda" acquired a negative connotation relatively late (20th century), mainly due to bad experiences with propaganda during the Second World War led by Nazi Germany. Today, the word is mostly used to denote manipulative or one-sided efforts to shape public opinion, often to promote certain ideological, political and economic interests.

"Religious frameworks for the development of the entire social life, and especially the emphasized function of religion in legitimizing and reproducing the system of government and social relations in ancient states, also determine the forms in which propaganda appears, until in the later development of certain states, primarily in Greece and Rome, politics and propaganda do not secularize and begin to appear in a pure form, as relatively independent entities" (Slavujević, 1997: 19). Propaganda today, which, ideologically speaking, is notorious (successfully replaced by marketing strategies, as well as public relations), in general, through the media, is aimed at the mass and is considered effective in shaping the psychology of the crowd, as opposed to the self-conscious individual: "[...] thousands of separate individuals can at certain moments, under the influence of certain strong emotions, as in the case of a large national event, acquire the characteristics of a psychological crowd. Under certain conditions, even half a dozen people can form a psychological crowd, while hundreds of people who have gathered by chance cannot form it. On the other hand, an entire nation can, without any visible accumulation, under the influence of certain factors, become a crowd" (Le Bon, 1989: 10).

In connection with this, a clearly expressed "propaganda intention" can be recognized already in the very beginnings of civilization. Namely, since the era of the first states, as well as political events within them, there has been an open intention of the ruling apparatus to influence the attitudes and actions of individuals and social groups. In this sense, a successful propaganda is one that manages to harmonize the cognitive and affective elements of systemic action from the point of view of power. The logic of reason, on the one hand, and the speech of emotions, on the other hand, combined, make attempts at manipulation particularly effective. Neither of these two "logics" is self-sufficient, just as neither of them unconditionally protects against manipulation; because, the use of Aristotelian logic in propaganda does not guarantee the truth, nor the acceptability of messages, while the separate use of "affective logic" does not necessarily mean manipulation, marked with a negative sign. Hard logical positions can also have an emotional component, and the propagandist, through various combinations, can influence behavior by using them.

Furthermore, considering this topic in the modern context, we can refer to the teachings of Edward L. Bernays, who is known as the founder of modern propaganda, that is, PR activities (public relations). In short, his principled position is that communication management (propaganda and PR activities) is necessary in modern democracies in order to avoid chaos and confusion. Although, nominally, every citizen has the right to decide on issues of public importance, as well as the way in which decisions on those issues are implemented, in practice this rarely happens. Because, if, hypothetically speaking, every individual was engaged in the study of economic, political and other areas of social life, and based on them made decisions, the state would function slowly and inefficiently. For example, Bernays claims that it would be desirable for everyone to be able to buy the best and cheapest goods offered on the market, but that in practice, if everyone individually checked prices and chemically tested products before buying, a real economic life would not be possible. In order to avoid general confusion, it is necessary for state institutions to narrow down the choice to those ideas and objects that attract the public's attention through propaganda.

In order to direct increasingly complex forms of life organization, new technical means were invented over time that supported the shaping and management of public opinion and communications. In the book "Propaganda" Bernays explains the structure of the mechanism that controls public opinion and talks about how it is socially desirable to devise an appropriate action strategy (manipulation) of a special representative who would try to win over the public for a certain idea, decision or solution (Bernays, 1928).

Bernays expresses this attitude by citing various examples from many spheres of social life, such as the economy, political action, education, art and science, etc., considering that the introduction of propaganda into modern democratic culture is inevitable, but it is also important to keep in mind the importance of preventing its abuse. Bernays also emphasizes the importance of technology, that is, technical inventions such as the steam engine and the printing press, on the one hand, and the importance of education, that is, the opening of public schools, on the other hand, which contributed to the strengthening of the civil class in the decision-making process.

In connection with the issues of ideology (education, and not only education, but also manipulation) Louis Althusser presented the thesis that the educational ideological apparatus is, in fact, the state ideological apparatus placed in a dominant position in mature capitalist formations, as a result of a violent ideological class struggle against the old, dominant state ideological apparatus (Althusser, 2009: 17). Althusser explained this thesis by pointing out that all state ideological apparatuses give the same result, which is a mere reproduction of production relations, that is, capitalist relations of exploitation. According to Althusser, education is not value-neutral, but is an ideological apparatus that serves to reproduce the prevailing social norms, values, and power relations. In a capitalist society, the educational system plays a key role in perpetuating cap-

italist relations of exploitation, by shaping people's attitudes, beliefs and behavior in accordance with the system's requirements. It goes without saying that Althusser, unlike Bernays, explored in a deeper and critical way the forms and structures through which the ideology of capitalism is transmitted through education, emphasizing the role of teachers as bearers of ideology and open propagandists of the capitalist order; he also underlined the fact that education is not just the transfer of knowledge, but it is primarily a means of controlling and reproducing socio-economic relations, for the purpose of exploiting the labor force in a capitalist-based order.

In contrast, Bernays presents the view that teachers should act in the education process both as pedagogues and as propagandists, and that each social group that occupies a certain position should accept an ideology that is in accordance with its role in a class society, regardless of whether it is the role of the exploited, exploiters, that is, of repression or professional ideologues.

Today, however, by advocating the idea that manipulation, propaganda and disinformation are things of the past, we can fall into error or, on the other hand, ask the question whether a democratic society is immune to them? Often, it is assumed (which is a belief unsupported by facts) that the audience recognizes the metalanguage of communication messages and manipulative discourses, which means that such content could not be defined as real manipulation, because the audience, that is, users of media content, are capable of interpreting the elements of manipulation. Contrary to such an opinion, it seems to us that the assurance that we are immune to ideological (media) content is the first step in the process of manipulation, because it is suggested to the interlocutors that they are free in their choices and opinions.

If we were to reduce manipulation to a way of using pure force, that is, limiting the freedom of those over whom it is exercised, then it would certainly be considered inhumane and ethically unjustified. Therefore, it is necessary to disguise it as one of the principles of organizing community life. "The most important, perhaps even the only strategy in manipulation is to limit as much as possible a person's freedom to discuss or oppose what is proposed to them. This strategy must be imperceptible, because otherwise the attempt at manipulation would be exposed. More important than the calculation that characterizes manipulation and the strategy it undertakes is the fact that it is hidden from the audience. The methods of manipulation must, therefore, be disguised" (Breton, 2000: 18).

Thanks to technological progress, manipulation strategies are taking on completely new forms, and warfare itself is getting a different concept and design. Masking and the inability to recognize serious non-military threats in hybrid warfare becomes an important security issue, and this type of threat is recognized as a complex phenomenon that finds increasing application in modern society. Theoretically speaking, this problem is of an interdisciplinary character, and multidimensionality is its basic characteristic. Non-military hybrid threats are complex operations that require an integrated

approach to solving security challenges. In addition, they can be demanding to recognize due to the variety and ability to quickly adapt to the current situation. Therefore, it is important to develop capacities and strategies for recognizing and countering these threats, both at the national and international level.

Furthermore, this phenomenon includes a combination of different tactics and strategies that are used to achieve the desired reaction or behavior of individuals or groups of citizens, all without the use of direct physical threats or violence. Manipulation in this context can include psychological pressure tactics, the use of disinformation, and propaganda, as well as the creation of fake news, scenarios or situations to achieve a desired effect. These manipulative techniques often include economic sanctions, diplomatic pressure, using media power to discredit or destabilize citizens, and other forms of vague or veiled threats. When these techniques are combined, a complex picture of manipulation is created that seeks to weaken the resistance or critical thinking of the target group, and to create a favorable atmosphere for the achieving of the manipulator's aspirations. It is important to note that these manipulative skills and techniques are usually not visible and require careful observation and analysis in order to be recognized and adequately responded to.

It is well known that the ideology of democracy is based on the principles of the rule of the people, respect for human rights, free elections, equality before the law, responsibility of the government towards citizens, etc. This ideology tends to create a political system in which citizens have an active role in decision-making, as well as greater control over the behavior of the authorities. Thanks to the systemic illusion in this organized ideological creation, we live in a world defined by the media (at least when it comes to Western cultures) which is far from reality. Along with the establishment and maintenance of democratic regimes, new technologies were developed that partly enabled us to renounce responsibility. Using technology uncritically, we fall into a vicious circle of a new way of controlling social layers, unaware that almost every connection we make to the network leads to a change in our attitudes. The thought of the fact that in addition to changing attitudes, affective and physiological transformations can also occur among users of social networks, leads to the idea that today we can significantly change our social paradigm.

We remind you that intensive research in the field of persuasion began at the beginning of the last century and is an integral part of social psychology. The definition of the term "persuasion" has never been clearly determined and many theories in the fields of psychology, marketing, rhetoric and similar disciplines have tried to explain what motivates people and changes their behavior in a predetermined way.

With the development of the digital sphere of communication, social interaction takes place in the cyber environment, and digital technology itself has occupied almost the entire space of our lives. Although the computer was originally created to process a

large amount of data, to facilitate work where a lot of time is necessary to perform it or to replace a human where a greater number of people are needed, that paradigm has been significantly changed in today's era. With the appearance of the interface, the computer becomes an indispensable medium that is used not only for business purposes, but also in free time; with the entry into mass use of portable smartphones, the cyber world is becoming a reality in which we live.

The sensory domain of this technology is potentially, as it seems, the most dangerous non-military threat to today's man. In the Clinical Research Laboratory of Stanford University, during 1997, Fogg and his collaborators started research in the field of interaction of technology with users, and changing their behavior patterns. It is, in fact, the very beginning of pioneering research, and the field is called "Captology", an acronym derived from the words "Computers as Persuasive Technologies". Fogg defines computer technologies used to change users' behavior patterns as "computer systems, devices, or applications that are intentionally designed to influence users' attitudes or behavior in intended ways" (Fogg, 2002).

Persuasion of users, in a planned and organized manner, and through certain computer programs can also be called "persuasive technology" or "persuasive design". This approach to technology involves the use of design techniques and strategies that are intended to influence users and encourage them to take specific actions or change attitudes, behaviors or habits. Persuasive design can be used for various purposes, such as encouraging users to use a certain application, to follow certain rules or guidelines, or to make certain decisions. This includes the use of visual elements, interactive functions, feedback mechanisms, as well as the application of the principles of social validation, authority or reciprocity, in order to achieve the desired change in user behavior. One of the key aspects of captology is the use of various strategies and techniques that target human instincts, emotional reactions and unconscious processes. They can be activated using visual stimuli, social proof, principles of reciprocity or authority, and other techniques used to achieve the desired response. For example, through the manipulation of user interface design or the use of certain language techniques, captology can target certain emotional reactions in users or encourage them to take certain actions, such as buying products, sharing content on social networks, or accepting certain ideas and attitudes. Along with this, it is possible to perceive the extremely negative potentials of captology that can be considered as non-military threats. The lack of transparency regarding the way in which technology is used to manipulate users, the absence of privacy protection or the potential abuse of such techniques in order to exploit or spread disinformation represent real threats not only in war, but also in peacetime.

To repeat, captology is a field of study in which new technologies are applied to predict the behavior and attitudes of users, and influence them, not only through computer-mediated communication, but also by directly influencing people. This discipline

focuses on the use of algorithms and programs that are intentionally created to cause desired effects on users' behavior and attitudes, applying psychological techniques such as rewarding, modeling targeted behavior or attitudes, as well as using emotional cues incorporated into the program itself. Examples of such tools include the use of different fonts and writing styles to attract attention or emphasize certain information, which is taken from political marketing in the press. Still, for example, bold text can draw attention to the importance of the content, while italicized text can indicate additional information that is not as important. Also, the addition of avatars in interaction with users can make them close in communication, while the development of artificial intelligence is rushing towards enabling increasingly complex interactions with users, which affect them emotionally. A similar situation can be seen in modern media, both traditional and digital, as D. Vuksanović talks about:

Certainly, it goes without saying that, although emotions are an integral part of the public media sphere, the rational approach of participating in public work should not be abandoned; it is only about the proposed reconceptualization of the public sphere that does not bypass affective experiences, but includes them in the context of rational action, that is, participation in public space. And although those media that operate within the entertainment industry and kitsch are certainly more inclined to exploit emotions in that area (sentimental novels, specialized women's magazines, tabloids that profit from news about celebrities, but also black chronicles, natural cataclysms, and, finally, terrorist attacks and reports from the battlefield), the border between informative media and those that serve exclusively for entertainment is increasingly permeable, and subjective and emotional journalism is more often represented in all media. In this sense, today's information does not strive so much for truth and presentation of facts, as, being of a commodity nature, it is aestheticized, even spectacularized and enriched with both an aesthetic and an emotional' dimension. (Vuksanović a, 2022: 151)

However, the question is whether technology serves us or we serve it, whether we are its products and how technology will use us in the future - these questions are becoming of great importance for our civilization. Captological tools and techniques successfully reduce the critical attitude and resistance of the user, encourage the desired reactions, acting on an unconscious level, that is, manipulating the user's emotions. Recognizing manipulative intentions, preventing them and improving legislation in this domain is of great importance, since the world we knew in the domain of traditional media has ceased to exist, and we do not recognize most of the threats that appear in the digital environment or do not have an adequate defense mechanism.

Among the most known (the most frequent) threats in the digital space are cyber attacks, identity theft, phishing, social engineering (manipulation of people in order to

reveal confidential information or perform some action, for example revealing passwords, accessing computer systems, installing malicious software, etc.), cyber espionage and violence, violation of privacy, zero-day attacks (finding weak points of existing software that are unknown to manufacturers or users, which allows aggression before finding solutions), then attacks on the Internet of Things (IoT) in order to control, spy or cause damage, and a combination of the previously listed threats with the aim of penetrating the system of a specific organization or attacking individuals, sabotaging infrastructure, such as energy plants, transport systems or communication networks... All this can have serious consequences for an individual and society as a whole. With the increasing use of artificial intelligence, there is a possibility that attackers can use AI to manipulate data, generate false information, or even automatically carry out attacks on computer systems. Furthermore, by introducing the use of biometric data (such as fingerprints, facial scans, pupils, etc.), there is an increased risk of theft or misuse of this data through hacking or compromising the system for storing it. Deepfake technology allows the generation of fake video or audio recordings that look and sound like they are authentic. These contents can be used to spread misinformation, extortion, blackmail, etc.

In addition to abuses related to the sale of information about users, the strengthening of new forms of censorship, the impermeability of mainstream media and most social networks to matters of truth, the persecution of prominent individuals who stand up for facts and the public interest, regardless of the political and existential consequences for them, their families and those who support them, artificial intelligence, which at first glance is 'obedient' and neutral, occupying an ever-increasing space in the media, does the rest of the work for corporations and thus increasingly alienates the media from their effective functions, turning them, in addition to exploiting data, into a tool for monitoring and control. It is, of course, a path of unfreedom, which can eventually turn into slavery. (Vuksanović, 2022: 184)

The captological influence of computer technology can, as we have repeatedly emphasized, be used to manipulate users' behavior through various techniques, such as psychological tricks, reward systems or personalized recommendations. This can lead to unwanted changes in behavior or addiction to digital platforms. At the same time, such abuses call into question the restriction of freedom of choice, because if computer technologies are used for systematic guidance or selection of users' choices, this can lead to a reduction of freedom (choice) and decision-making autonomy of the individual. Such situations are especially problematic if they are used to impose certain political or ideological positions. In addition, the use of computer technologies to personalize content can lead to the creation of digital ecosystems that expose users to only certain attitudes or information, which can significantly lead to the polarization of society.

Legal regulation that predicts and limits, and sanctions the misuse of computer technologies to change human behavior may be insufficient, because it is difficult to set clear boundaries between useful and harmful use of technological knowledge. In such a situation, there may be a lack of adequate regulations for the protection of users, and they may be exposed to various abuses. The influence on the unconscious of a person through captological algorithms is difficult to recognize. Furthermore, we can ask whether research on the misuse of captological tools today is beneficial, especially if it is viewed from the perspective of those who hold most of the capital in their hands.

(...) reflecting in the spirit of transhumanism, the current/future man, as claimed by Klaus Schwab, is conceived as a 'fusion' of physical, digital and biological 'spheres' of living. This is really about the continuous integration of the listed components into the concept and practice of the new man (as a species), which will be enable by new technologies (Schwab, 2022). That process, as it seems, has already begun in a big way, and it is in line with the socio-economic changes that formed a completely different reference frame - the so-called. digital capitalism, which serves as a prelude to the anticipated Fourth Industrial Revolution. (Vuksanović, 2023: 140)

Given that we cannot observe non-military hybrid threats separately from the ruling ideology, studies on the subject of digital capitalism can give us clues about how and in what way to recognize such threats and adequately react to them. Since, the ideology of digital capitalism has a decisive influence on the way in which digital technologies are used, developed and regulated in modern society; at the same time, from that (critical) viewpoint, numerous questions can be asked about privacy protection, legal regulation and social justice in the digital age.

Certainly, the ideology of digital capitalism advocates the application of digital technologies in the context of the capitalist economic system, and basically, this ideology promotes technological progress, innovation, competition and entrepreneurship as key factors in the development of society. Different digital platforms should enable easy business start-up and connection to the market, creating new opportunities for economic growth; however, the issue of data abuse and social inequality, as well as the practice of manipulating the public sphere, are essential for modern man.

The new ideology also brings with it a phase of transition from the era of humanism, enlightenment, industrial revolution and information era to the time of more ubiquitous implementation of transhumanism, in all spheres of life. This controversial movement is focused on human superstructure through technological innovation, gradually increasing humanity's potential, while also considering the future related to the development of artificial intelligence. Not so long ago, from the beginning of the 20th century, technological progress had a humanistic sign, facilitating work processes and freeing up time for individual needs. "However, after several years of socio-economic change, technology grad-

ually nurtured its transhumanist goal of making humans better for the world now."

If the transhuman entity can be seen as a transitional form between a human being and a potentially more advanced form of existence, posthumanism, as a concept and ideology, goes one step further by striving to create beings that have completely surpassed human limits and become fundamentally different in terms of characteristics, abilities and identity. This term encompasses the idea that technological, biological or other prostheses could lead to the creation of new species that are no longer limited by human biological or cognitive frameworks. The posthuman being, therefore, can take various forms of appearance - from biological entities with enhanced genetic characteristics to artificial intelligences with superior cognitive abilities. Certainly, this topic includes a wide range of ideas and speculations about possible forms of warfare of the so-called posthuman beings.

To conclude, as a nascent discipline, captology develops both independently and alongside wars, and it is not excluded that the military industry also uses it for propaganda purposes, as it did when it came to radio, television and the Internet. Given the fact that captology is based on knowledge from the fields of applied psychology, neurophysiology (medicine) and modern programming and engineering, it is suitable for use as a preparation for wars, a kind of logistical support for psycho-physiological strengthening of war actions, and characteristic forms of manipulation that can be realized in technologically highly developed civilizations, both in wartime and in the so-called peacetime living conditions. Namely, it is one of the tools that can be used to ensure continuous warfare. Based on traditional propaganda, techniques of shaping public opinion and mass management, this tool has another "quality". Namely, it can be the "invisible" enemy that shapes our consciousness, but it equally affects our unconscious, i.e. psycho-physiology. From the point of view of media and technologically insufficiently trained ("literate") users, captology can be a reliable basis and means of war actions that belong to non-military activities. In other words, captology can turn from a tool into a weapon, the effects and activities of which are difficult to recognize, and besides, they cannot be completely controlled. Broadly speaking, captology can have a significant effect on the conduct of modern propaganda wars, whereby knowledge and skills taken from modern psychology, medicine (neurology and neurophysiology), marketing, PR, as well as the art of programming are interdisciplinary unified into one of the means by which modern wars are waged. This discipline can simultaneously become a theoretical basis and a practical instrument of the war of all against all (Hobbes), thanks to the connection of knowledge from the fields of biology, medicine, psychology and technological skills; it can also, without shedding a drop of blood, become a means of gaining power and maintaining control over the oppressed.

It is known, ever since Bacon (up to Foucault), that modern knowledge is connected with instances of power and that wars based on knowledge (technology associ-

ated with the former social-humanistic sciences, as well as new knowledge) colonize the little humanity and privacy that is left to humanity. Although captology is not necessarily a means of manipulating technology (although it is always already in the service of capital), in the context of its possible and real abuse for war purposes, its application should be taken into consideration when it comes to security. Also, ways to regulate and channel its effects should be explored so that they are relatively acceptable, in order to avoid the numerous risks of instrumentalization of captological tools, as well as the mechanisms of their abuse.

REFERENCE LIST

- Altiser, L. (2009). *Ideologija i državni ideološki aparati* (Beleške za istraživanje), Karpos.
- Bernays, E. (1928). *Propaganda*, 10.12.2012. <http://wikisbooks.com/w/images/1/1f/Propaganda.pdf>.
- Breton, F. (2000). *Izmanipulisana reč*. Beograd: Klio.
- Fogg, B.J. (2002). *Persuasive Technology: Using Computers to Change What We Think and Do*. Ubiquity.
- Le Bon, G. (1989). *Psihologija gomila*, Zagreb: Globus.
- Slavujević, Z. Đ. (1997). *Starovekovna propaganda: Od Vavilonske kule do "Panem et circences!"*, Institut društvenih nauka, Beograd:Radnička štampa.
- Vuksanović, D. (2022). Estetika, emocije, kultura i mediji, in: *THEORIA* 65 (2), Filozofsko društvo Srbije, Beograd, pp.145-158, <https://doi.org/10.2298/THEO2202145V>, p.151.
- Vuksanović, D. (2022). Mediji i sloboda: osnovna pitanja, *CM, COMMUNICATION AND MEDIA*, Vol XVII № 2, Fakultet političkih nauka, Beograd, pp. 183–199,
- Vuksanović, D. (2023). Mediji i budućnost: pametni gradovi, ljudi i zajednice. in: *Zbornik radova Fakulteta dramskih umetnosti*, No.43, Institut za pozorište, film, radio i televiziju FDU, Beograd, pp. 135-148,

Nemanja Stevanović¹

Marija Mićović²

Dušan Radulović³

CYBER DEFENCE STRATEGIES OF MILITARY NEUTRAL COUNTRIES – CASE STUDY: SWITZERLAND

Abstract

Strategic solutions that should contribute to the security of cyberspace are of great importance for the entire security and defense system of the country. The challenges of the technological revolution and the rapid development of information technologies have created new risks and threats of a non-military nature, so the very national security of modern states largely depends on a quality strategic framework that regulates this area. Adequate strategic framework contributes to prioritization and organization, as well as control of national vulnerability to critical information infrastructure. As the defense systems of the member states of military alliances are implemented in accordance with the standards and regulations defined at the level of these alliances and in order to contribute to the collective defense of such a community, the challenges of militarily neutral states, which have no obligation towards other subjects, and that is the case at allied relations, are even more pronounced. On the one hand, they are left with free space for maneuver, so they can develop their cyber defense strategies in accordance with the concrete security challenges, risks and threats of their country in cyberspace, while on the other hand, their vulnerability is increased by the very fact that most of these countries do not have the protection mechanisms available to wider allied communities. Accordingly, the scientific goal of the paper is a scientific explanation of the contribution of cyber defense strategies to the complete security and defense system of militarily neutral states, whereby the Swiss Confederation was chosen as an example, according to its efforts in this field.

Keywords: *cyber security, strategies, defense, Switzerland, neutrality.*

INTRODUCTION

Archetypal patterns of behavior, as a result of accumulated experience about the inevitable, existential need for a state, for the existence of traditional armed forces, as the only sustainable and, above all, primary instrument in confronting challenges, risks

¹ Faculty of Diplomacy and Security, Belgrade, Serbia, nemanja.stevanovic@fdb.edu.rs

² Criminalistic and Police Studies University, Belgrade, Serbia

³ Ministry of Foreign Affairs of the Republic of Serbia, Belgrade, Serbia

and threats to security, and which have been established as the foundation of the defense policy of almost all subjects of the international community, are responsible as the ideological creators of an attitude that is no less significant and ubiquitous today, which resists the long-standing global demand to abandon the realistic military approach and adapt it to the authentic characteristics of the modern era. The striking features of the current moment in the history of humanity, contained in the specifics of intensive innovations, also carry with them major socio-economic changes, which are not only visible in the economy, business, culture, but also in other areas that the adoption of new technologies has encouraged to change. The technological revolution, also very important in the military sphere, has contributed to the advancement of artificial intelligence, robotics, genetics, renewable energy and many other fields, which has allowed innovations of this kind to transform the world and change the way it functions.

Responding to the demands of the modern era, reflected in the change in the security paradigm in the post-Cold War period, without abandoning the traditionalist approach to understanding the role of the armed forces, the military industry, although still reserved, is implementing technology and making a clear turn with an indirect impact on military capabilities and strategies of importance for effective response in cyberspace. Therefore, technological progress in the military sphere has caused consequential changes in military doctrines, strategies and tactics, and in order to maintain a military advantage, armies around the world are constantly monitoring and applying the latest technological developments in their operations. In an effort to adequately confront the security threats they face, and with the aim of establishing regional and international stability, states create their own defense policy that is adapted to the collective defense treaty, if it is about states that are members of military alliances, or primarily to national defense interests, if it is about states that have opted for the concept of military neutrality. However, when considering the future nature of warfare, the sustainability of the concept of military neutrality is questioned. The armed forces of many countries around the world are adopting a doctrine of multi-domain operations, which requires the coordinated use of military capabilities in multiple domains such as air, sea, land, space and cyberspace, but also the ability of allied countries to do so together and quickly. Essential elements for these highly complex military operations are intelligence, surveillance, reconnaissance and other types of data collection using multiple sources such as satellites, unmanned aerial vehicles and operations in cyberspace that are fed into command, control and communications to create a sophisticated picture of the battlespace or the overall strategic environment. Given the relatively limited capabilities of European armies, information sharing among allied armies will be crucial for future military effectiveness⁴, but it would also mean that the armies of neutral countries would be largely excluded from these arrangements.

⁴ Classification issues and a general lack of trust make it difficult for NATO members to share sensitive tactical data in real time with Austria or Ireland in a military crisis. Even without a crisis, neutrality already makes it difficult for some NATO members to share data with these countries on an ongoing basis – for example, about cyber threats.

The vulnerability of militarily neutral states in terms of responding to new forms of threats that are being established in the cyber domain is primarily reflected in the lack of access to protection mechanisms developed in broader allied communities. Where the concept of military neutrality is a substitutive element of national identity and national history, which effectively contributes to the stability of the country, which distinguishes the state that is the subject of the case study of this paper – Switzerland – from the standard model, there is also a modality of developing a defense and security system that demonstrates a willingness to effectively resist the ever-growing potential of virtual threats.

THE CONCEPT OF MILITARY NEUTRALITY IN THE CONDITIONS OF THE CHANGED SECURITY PARADIGM OF THE 21ST CENTURY

The unipolar global order constructed on the basis of the supremacy gained by the United States through its victory in the Cold War, built a noticeably different global geopolitical architecture during the last decade of the 20th century. The transformation of the concept of national security, which until then had steadfastly required an immanent state-centric approach and the inclusion of other referent security subjects in the subject of research of this concept, further caused a change in the understanding of the very nature of security threats. Resisting the demands of theorists who pioneered this concept, such as Hans Joachim Morgenthau and Kenneth Waltz, who recognize exclusively military challenges, risks and threats to security, and under the enormous influence of the Copenhagen School of Security Studies, the subject of study of security sciences also included non-military challenges, risks and threats to security. The conditioned change in the security paradigm of this kind has also created certain changes in the way of thinking, strategies or approaches to the issue of security at the national, regional and global levels. The growing potential of specific security threats for the 21st century, such as terrorism, hybrid wars and cyber threats, has also conditioned the transition from classical to asymmetric security threats, which have annulled the hierarchical order of military and non-military challenges, risks and threats and pointed to the equally dangerous existence of threats on both spectrums. Further progress in information technologies has reiterated the demands for the transformation of the security paradigm, but has also created a new space as a testing ground for the manifestation of security threats, which at the same time "represented a kind of turning point in the sphere of military activities... and provided great opportunities for conducting special propaganda operations as well as carrying out attacks via computer networks on enemy information and communication systems" (Putnik, Milošević and Bošković, 2017: 176). The change in the security paradigm, accordingly, requires the adaptation of policies, strategies, resources and management mechanisms in order to respond to new forms of threats, which are also significant from the perspective of national security and defense policy because

they are aimed precisely at national critical infrastructure. Since innovative technologies are a specific feature of the period of transformation of the security paradigm, cyberspace has become part of the same infrastructure. As Mićović states, in modern conditions, "key infrastructures have become an integral part of cyberspace and play a vital role in supporting many of our daily activities (including travel, water and energy use, financial transactions, telecommunications, etc.)" (Mićović, 2020: 10).

In a context where the new changes characteristic of the current century, especially those in the field of cybersecurity, have so radically altered almost all concepts of security, the dilemma arises as to how sustainable the concept of military neutrality, in its original form, really is. Establishing the rights and duties of countries that avoid war when conflict affects their environment is a long-term and constantly renewed European process. The ambition to curb the violence of war requires dialogue between states, and in this sense expresses an international desire in line with the prospects for peace. Some periods, such as the second half of the eighteenth and nineteenth centuries, were marked by a collective assertion of the fundamental rights of neutrality, which did not always withstand the temptation of major conflicts (Devine & Agius, 2011: 266). Although the principle and practice of non-war have been regularly criticized, they have never disappeared, demonstrating an enduring belief in the possible coexistence of war and peace. Unlike non-war, which is the state of affairs, neutrality entails rights and duties. The history of neutrality is one of continuous efforts to contain the devastation caused by war, by establishing a fair balance between the right of a belligerent party to harm its enemy and the right of a neutral party to avoid the consequences of a war in which it is not involved (Müller, 2019: 188). This balance, however, does not mean that neutrals can continue their activities without being affected in one way or another by the international situation.

Although the term "neutral" was not used in its political sense until the late Middle Ages, situations of neutrality consisting of compromises between belligerents and non-belligerents certainly existed before that period. The inclusion of the rights of neutrals in Western legal doctrine was the work of the legal scholar Hugo Grotius, who addressed the subject in some detail in his *Law of War and Peace* published in 1625. In practice, in exchange for their impartiality and abstention from conflict, states claim the right of impunity for their territory, as well as the security of their trade and navigation (Vetschera, 1985: 56-57). Nevertheless, every conflict leads to disputes between neutrals and belligerents over recurring issues, the most prominent of which concerns the definition of what constitutes participation in war. Tensions with the belligerents encouraged neutrals to unite in defense of their rights, as in the First League of Armed Neutrality in 1780 (Müller, 2019: 41). The legal framework for neutrality did not withstand the test of either the French Revolutionary Wars or the French Empire. The determination of the belligerents to reduce the foreign trade of their enemies as much as possible gradually limited the rights of neutrals. In addition, it was a period rich in reflections on maritime law and disputes with

countries avoiding conflict in order to ensure the security of their commitment. This was especially the case for the United States of America, which demanded freedom of neutral trade in the name of the principle of European law of nations (Neff, 2022).

During the nineteenth century, neutrality played a central role in the international system. It was praised and promoted by both small and great powers, and was the subject of reflection by international legal experts. The Paris Congress of 1856 established rules governing neutral trade in times of war. In the decades that followed, the framework of neutrality was gradually clarified through modifications of international law and evolved in accordance with power relations, advances in military technology, and the culture of peace. The practice of neutralization allowed certain territories (the Black Sea, Switzerland, Belgium, Congo) to be removed from international competition, thereby contributing to the stability of the international system (Neff, 2022). However, the great powers found themselves in an ambiguous position regarding neutrality, as they participated in its definition and claimed its prerogatives when not at war, but sought to limit its scope when at war. The promotion of neutrality during the nineteenth century also relied on pacifism and legal positivism, which cherished the hope of containing the consequences of war, as demonstrated by the recognition of the immunity of the Red Cross, as well as of medical personnel and equipment. Clarification of the neutrality regime was on the agenda of the Second Hague Peace Conference in 1907, attended by some 40 countries from Europe, America and Asia. Among other things, they agreed to constitute a genuine international legal framework for the rights and duties of neutrals.

World War I began with the entry of German troops into Luxembourg and Belgium, despite the fact that their neutrality had been guaranteed by the continent's great powers. Over the following months, the legal construction of neutrality collapsed in the face of violent attacks on the law by the belligerents. The expansion of the concept of smuggling, the implementation of the Allied blockade, and submarine warfare made it impossible to maintain a *de facto* neutral position. The United States, which had officially entered the war in April 1917, adopted certain measures that it had previously declared detrimental to the rights of neutrals. The first global conflict was a hard lesson for those who believed in the possibility of containing the violence of war. After 1918, both the law and the principle of neutrality were subject to sharp critical examination. Opponents of neutrality denounced the indifference of those who remained selfish observers of the tragedies unfolding before their eyes, with the ambiguity that allowed them to exploit the situation to enrich themselves, and the delusion of their positioning in the context of large-scale wars that inevitably involved all countries. Collective security, which led to the founding of the League of Nations in 1919, limited the space for neutrality by forcing its members to impose sanctions on a state deemed guilty (Danspeckgruber, 2021: 251). However, during the 1920s and 1930s, the principle of abstention from war regained force under the leadership of non-League of Nations states

that demanded the right not to be involved in a conflict against their will.

The Second World War marked a new degradation of neutrality. In 1939, about twenty European countries declared their neutrality, although only six remained out of the war by 1945. The German invasion, pressure from Berlin, and vested interests pushed numerous countries into the conflict. Moreover, the configuration of the war made it very difficult to fulfill the basic duties of neutrality, restraint, and impartiality. Therefore, it is more accurate to speak of "non-belligerence"⁵ (non-belligerent party), which included states from both Europe and the American continent (Neff, 2022). The Second World War marked the legal breakdown of neutrality, since relations between countries that participated in the war and those that abstained were no longer based on a common referent. As a result, the abolition of neutrality laws, in the context of the reorganization of international relations under the auspices of the United Nations, is not surprising. Since 1945, increasing forms of confrontation and belligerence, together with the increase in trade and international traffic, have made it difficult to apply the law of neutrality that regulates the intermediate state between war and peace. As a result of non-alignment, isolationism, the right to intervene, participation in international military operations, the increasing rarity of declarations of war and conflicts with non-state actors, Europe and the world have entered a period of post-neutrality, the contours of which still await precise definition.

The concept of military neutrality in the context of redefined defense strategies, which emerged as a result of adapting to newly emerging forms of threat, has lost its already vaguely defined orientation. Policymakers today advocate a hybrid model of military neutrality - abstention from joining military alliances that is compatible with security and defense cooperation with the EU and NATO, because such cooperation is necessary to address the security challenges of the 21st century. As we have seen, the roots of neutrality lie in the idea of non-war, a concept that implies not participating in or being drawn into wars between other states. Neutrality, in this sense, was a protection for states: by committing not to join a war between others, a state hoped to avoid attack by those states or at least to protect the use of its territory. One of the rare examples of an adequately conceived concept of military neutrality is the very state that was chosen for the case study in this paper for the same reason – the Swiss Confederation. For centuries, the small Alpine nation of Switzerland has adhered to a policy of armed neutrality in global conflicts. Switzerland is not the only neutral country in the world – there are also Ireland, Austria and Malta, all of which take similar non-interventionist positions. However, despite the existence of several other similar examples, Switzerland remains the oldest and most respected, which has always attracted expert attention summarized in the question: How did it earn its unique place in world politics?

⁵ A non-belligerent is a person, state, or other organization that is not fighting in a given conflict. The term is often used to describe a country that is not participating militarily in a war. A non-belligerent state differs from a neutral state in that it may support certain belligerents in a war, but is not directly involved in military operations.

CYBER DEFENSE STRATEGIES IN THE CONDITIONS OF PROCLAIMED MILITARY NEUTRALITY

The military industry faces a series of challenges arising from the complex nature of international politics, technological innovations, economic factors and conditioned changes in military doctrines. Rapid technological progress has created great pressure on military industries to adapt their resources to the demands of the new market in order to keep up with the competition. New forms of application of technologies for military purposes, such as artificial intelligence, autonomous vehicles, unmanned aerial vehicles and others, have placed new demands on the defense policy of almost every country for investment in research and development. Precisely for this reason, in order to maintain the presence of their military power at the regional or global level, many countries in the world have increased their investments and significantly expanded the scope of military budgets, which can consequently affect the development of other forms of threats, such as the development of the gray market (Knežević et al., 2021).

The changing nature of security threats has also had a direct impact on all levels of the logistical and organizational structures of the armed forces.⁶ The military, as part of the national critical infrastructure, is significantly more exposed to cyber attacks that have obvious consequences for their operational capabilities, but also for trust in military systems and their operability. In addition to the complexity of the threats themselves, “the incredible complexity of infrastructure systems is definitely the biggest common problem of all countries that have embarked on the analysis and identification of critical infrastructure, as well as those that are trying to form a policy for the protection of critical infrastructure” (Mićović, 2015: 376). Protecting, first of all, military and then other critical national infrastructure from cyber attacks requires the implementation of various security measures, including new strategic orientations, security protocols, cryptography, network surveillance, training of military personnel, as well as continuous monitoring and timely response to potential threats. In addition, cooperation between military intelligence and security services, as well as civilian security services in the exchange of information, which must be provided for by special strategic solutions, is of crucial importance for strengthening defense against cyber attacks and ensuring the operational capabilities of the armed forces.

Future conflict will involve sophisticated cyber warfare, and countries around the world have recognized the strategic value and advantage of investing in both offensive and defensive cyber capabilities. In this sense, cyber defense strategies are now a critical tool for defending a nation’s vital defense assets. A strategy of this type details how a mil-

⁶ Since the Russian cyberattacks on Ukraine began in 2014, they have shown that conflicting actors will not hesitate to use cyber operations – including disinformation campaigns (propaganda), espionage, and the disabling of essential services and critical infrastructure – at any time, up to and including combat operations.

itary system will combat cyber threats and ensure that its capabilities remain out of range of enemy attacks. At the same time, it represents a path to effective cyber-resilient defense and contains proclaimed goals and principles for maintaining a strong cybersecurity posture in a changing strategic environment. One of the crucial issues, which the strategic guidelines themselves should foresee, is cooperation with other states in the areas of protection against cyber attacks, such cooperation being compatible with the status of military neutrality. However, a strategic document in this area must be particularly careful and precise, because it is evidently a delicate area where military and any other dependence can very easily arise, which ultimately undermines the very credibility of neutrality among those states that have chosen it as their military commitment (Dahinden, 2021: 10). However, while joining a defense alliance is not compatible with neutrality, the exchange of experiences, cooperation in training and armaments are without any doubt, and this is precisely the basis of the framework on which the cyber defense strategy of a militarily neutral state can and must be based. The world is therefore faced with long-term requirements for the strategic shaping of defense tactics for responding in the event of a cyber attack on military and civilian critical infrastructure. Whether these states are militarily neutral or members of collective defense treaties, the threats that come from this area and that are increasingly pronounced and destructive every day are something that they must deal with without distinction. However, the approach to the conception of cyber defense strategies differs between militarily neutral states and those that are not. Militarily neutral states, in keeping with their commitment to rely solely on their own resources and capabilities for defense and protection, must also take a more proactive approach in designing cyber defense strategies. This requires a shift from a mentality of relying solely on them to deterrence through denial (persuading an adversary not to attack by convincing them that an attack will not achieve the intended goal) (Kelsey, 2008: 1437).

Instead, these states, when designing a strategic framework for action in the defense and protection of cyberspace, are required to implement a completely new way of thinking about how to operate, compete and, if necessary, fight in the cyber domain. The first step is to adopt a comprehensive approach to cyber defense. This requires better integration of activities among the many actors at each of the three levels of cyber defense: political, military and technical (Jensen, 2011: 838). At the political level, militarily neutral states must be proactive, shaping cyberspace in accordance with their own interests and values, promoting stability through the development of future-oriented policies and by promoting support for international norms, while clearly signaling to adversaries that there is a readiness to respond quickly. At the military level, it is necessary to strengthen the role of its military cyber protection entities by enabling civil-military cooperation during peacetime, crises and conflicts. At the technical level, it is necessary to strive for effective defense, ensuring resources and sufficient equipment to detect and prevent malicious cyber activities.

Cyber military strategies, on the other hand, must give sufficient importance to intelligence activities. This is very important because in this way they support intelligence operations and contribute to mechanisms for raising awareness about the security situation in the country. The military strategy should also have elements dedicated to efforts to build operational capacities that are necessary for such a system to counter cyber threats. Capacity building can be considered one of the prerequisites for primarily offensive measures, since it would be almost impossible to build effective offensive measures without building qualified military teams and structures. Likewise, offensive measures also represent an effective means of deterrence (Huang & Zhu, 2019: 53). Therefore, as a result of the above, two important and almost substitutable elements of a cyber defense strategy are offensive measures and deterrence measures, the effectiveness of which in protecting military systems depends to a certain extent on the effort invested in building the capacities themselves.

MILITARY NEUTRALITY OF THE SWISS CONFEDERATION AS A BASIS FOR DEVELOPING A CYBER DEFENSE STRATEGY

Cyberspace has become an increasingly challenging area in recent years, with cyberattacks being carried out on all critical infrastructure targets, without exception. As such, cyberattacks are recognized as one of the tools used for competition, intimidation and coercion, as recognized by the European Union's security strategy, with this qualification also implying that the distinction between war and peacetime is increasingly narrowing. The devastating and exhausting war for the future of Ukraine has raised uncomfortable questions in many European capitals, including those whose states clearly declare themselves to be militarily neutral. In Switzerland, a traditionally neutral and peaceful nation, the war has revived an old debate about neutrality, arms exports, and Swiss national security. In adopting sanctions against Russia, Switzerland has acted with more impartiality than in decades before, but it has also been cautious in its approach, and the principle of neutrality remains popular with the Swiss public (Steffen & Patt, 2022: 3). The long-standing concept of armed neutrality is instilled in every Swiss citizen almost from birth.

Politically, it is largely uncontroversial issue and is supported by a consistently high percentage of the population. The Swiss army and professional air force guarantee that the country's neutrality and independence can be enforced and that they also provide a certain deterrent effect. Seemingly positive experiences from the past have strengthened many Swiss in the belief that neutrality has helped their small country in the center of Europe to prosper, stabilize, and be at peace over the past centuries. Switzerland has survived two world wars largely intact. Especially since World War II, neutrality has become a powerful myth, shared by a large part of the population, regardless of political ideology. Swiss voters of almost all political views believe in some kind of neutrality dividend.

When it comes to developing an effective response system in the event of cyber attacks of various kinds, the Swiss authorities have established an institutional apparatus responsible for the implementation of this work - *The National Cyber Security Centre* (NCSC). This body was established in 2020 and is the Swiss centre of competence for cybersecurity and therefore the first point of contact for businesses, public administration, educational institutions and the general public on cyber issues. It is also responsible for the coordinated implementation of the national strategy for protecting Switzerland from cyber threats. *The Reporting and Analysis Centre for Information Assurance* (MELANI), together with the national *Computer Emergency Response Team* (GovCERT), are integrated into the NCSC and together they form a centre of technical expertise that will be further expanded in the future. Traditionally militarily neutral Switzerland adopted a new *National Cyber Strategy* (NCS) on 5 April 2023. The strategy sets out the objectives and measures by which the federal government and the cantons, together with the business community and universities, intend to counter cyber threats (NCS, 2023). The strategy also provides for the establishment of a Steering Committee to plan and coordinate the implementation of the strategy, as well as to refine it. Its role is to expand and increase its independence. In order to increase Switzerland's resilience and effectively counter cyber threats, cooperation between the federal government, the business community, the cantons and universities is essential. The new cyber strategy approved by the Federal Council and the cantons, which replaces the previous strategy, establishes a framework for this and defines common goals and measures. Switzerland has already successfully implemented many measures since the first cyber risk protection strategy was launched about a decade ago. For example, the federal government has continuously expanded the responsible organizations and created sustainable structures.

An analysis of the Swiss Confederation's strategic framework, which regulates this area, indicates the existence of three main measures to increase awareness of the importance of cybersecurity and build more resilient defense systems:

- Early recognition of current innovation trends and technologies and development of education about them - trends and technologies in the technical-technological sector, as well as the resulting opportunities and risks that may arise, must be identified at regular intervals and at an early/initial stage. The results of this monitoring are communicated to stakeholders in scientific research organizations, the private sector, the public sector and society. Basic and applied research is promoted as needed and to the extent possible within existing funds and processes (e.g. through national research programs).
- Expansion of the educational framework and promotion of competence building - in an exchange involving the private sector, universities, the federal government and the cantons, the need for competence building in the field of cybersecurity is analyzed. In particular, it is examined how the topic of cyber-

security can be increasingly integrated into existing courses and study programs.

- Creating a favorable framework for an innovative information and communication economy in Switzerland; the country should be an attractive location for companies in the field of ICT security. Increased exchange between the private sector and research should help promote innovative start-ups in this field. In cooperation with associations and universities, further measures to improve the framework for the ICT security economy will be examined and implemented as needed.

The existing measures envisaged by the aforementioned strategic framework are a direct response to research conducted in recent years, which has indicated the need to make a greater contribution to raising awareness of cyber threats among the population, businesses and policymakers and to undertake additional activities in terms of informing about possible protective measures. Communication guidelines, responsibilities and processes are also defined in the aforementioned Strategy. It also discusses the balance between confidentiality and the need for information. The implementation of the envisaged concept through media and public relations should be specific to the target groups and actively promoted. The same framework also stipulates that the federal government should aim to help raise public awareness of cybersecurity and defense, to strengthen communication about cyber threats and to use the existing capacities of associations and institutions already active in this area.

The existing strategic framework for cybersecurity in Switzerland, which also includes provisions relating to the strategy for defending the country against threats of the same type and nature, ensures that cyberspace plays an increasingly important role in military affairs and tasks. The quality of the outcome of these affairs and tasks largely depends on how well decision-makers understand today's cybersecurity environment and how prepared they are to build adaptable systems to meet all the challenges that lie ahead. To this end, the Swiss Confederation's strategic preoccupation explicitly highlights five points that illustrate the current state of affairs and at the same time contain guidelines for building an adequate cyber defense system: first, cybersecurity implies continuous work on digital transformations, according to which numerous organizations, including the military industry, must incorporate comprehensive technologies into their systems and processes (Baezner & Cordey, 2019). When it comes to establishing cybersecurity as part of the modernization process, Switzerland should make additional efforts in this field in order to introduce certain and necessary changes. The vulnerability of their systems was demonstrated by various cyberattacks in the summer of 2023, when the websites of the federal government and state organizations such as the Swiss Federal Railways, the Swiss Post, and the cantonal administrations in Zurich, Basel, and Geneva

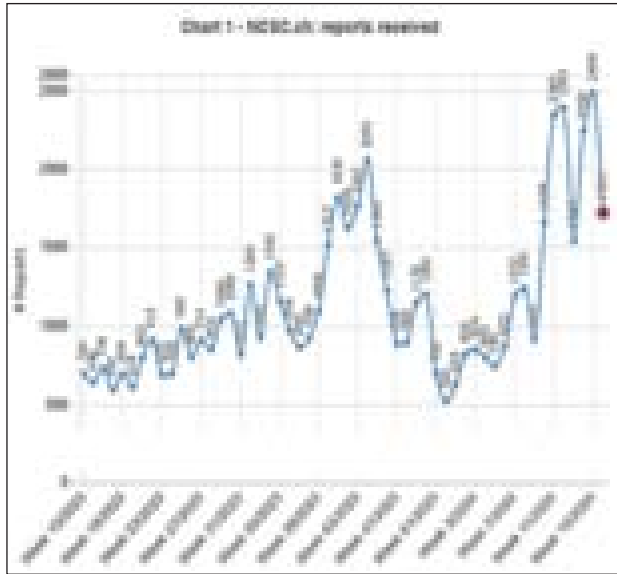
were brought down by DDoS attacks.⁷ Modernization and replacement of old systems must therefore be a constant priority. Cybersecurity must not be an afterthought for organizations when deploying new systems and upgrading old ones; secondly, the need to find and properly train cyber experts is becoming increasingly evident, and a cost-effective approach of this kind is more beneficial in the long term than short-term outsourcing (Fischer et al., 2023). The lack of cybersecurity experts also remains a problem for the Swiss authorities. According to the global association for certified cybersecurity professionals, there are 4.7 million cybersecurity employees worldwide, but an additional 3.4 million are needed (ISC2, 2022). With this in mind, the Swiss military has launched its own personnel policy to train and develop adequate personnel, who should be able to recognize, detect and act early in the event of cyber threats directed at the military structures of this country; third, proper guidance by all relevant factors of the given system remains a major challenge, as this can strengthen more consolidation and centralization of responsibility; fourth, funding is the fuel that drives the development of adequate systems capable of responding to all types of threats in the virtual space. A centralized and simplified budgeting process facilitates the allocation of financial resources in a reasonable manner; fifth, cyber defense with a clear mission is becoming increasingly important and must include command, control and communication and a well-defined leadership structure. The Swiss defense system has made good progress in the areas of management, investment and planning in recent years. With the establishment of the National Cyber Security Center (NCSC) in 2020, the Swiss government created a central point of contact for authorities, educational institutions, businesses and the general public on cybersecurity issues and established a group of experts to support departments and administrative bodies with the development and implementation of cybersecurity standards. The transformation of the NCSC into a federal office in 2024 further strengthened the governance of the cyber domain within the government. Thus, cooperation in the field of cybersecurity already works quite well at the national level, but the Swiss federal system makes the situation more difficult at the cantonal and municipal levels. The efforts of various cantons (including Zurich, St. Gallen and Basel) to invest more in cybersecurity and establish their own cantonal cyber defense centers represent an important step towards the predefined goal arising from the strategic framework.

Although not one of the countries with the highest risk of cyberattacks, Switzerland's defense has shown all its system vulnerabilities in recent years, which places it behind many countries in Europe (those that are not militarily neutral). In 2022 alone, the National Cyber Security Center documented more than 34,000 attacks, which shows that the numbers have tripled since 2020. The downward trend in cyberattacks in recent

⁷ DoS or DDoS is a hacker attack that, in simple terms, boils down to exhausting the resources of a service on the Internet, thereby making it unavailable to intended users. It disables a network, computer, or other part of the infrastructure in such a way that users cannot use it.

months in Switzerland (Figure 1) (NCSC, 2024) is a direct result of the new measures prescribed by the revised strategic framework from 2023, which shows that the defense capacities, capabilities and defense power of the Swiss Confederation in this regard are further advancing and that the formula for success in this field lies precisely in strengthening the strategic framework from which the necessary elements for building an adequate system are drawn.

Figure 1. *Trend of cyberattacks in Switzerland for the period 2023-2024.*



CONCLUSION

The multipolar global environment, polarized in relation to all indicators of the distribution of power and wealth, in a very characteristic moment in the history of humanity, imbued with its authentic specificities shown in the process of globalization and the progress of innovations, has highlighted the strategic and importance of any other kind in terms of the commitment to the concept of a country's defense policy. The complex geopolitical architecture of the world and the socio-economic prerequisites for greater prosperity have directed most subjects of the international community to embrace those actors in whom they believe that belonging to a chosen collective instills confidence and guarantees stability and security on the path to achieving national, regional and global goals or even claims. On the other hand, outside the interesting embrace of friends as needed and depending on the goal, believing that even confidence in one's own superiority and supremacy is a formula for success, only a few states remain, among which the Swiss Confederation stands out due to the numerous characteristics listed above. The neutrality of Switzerland, the very core of its identity, from this point of view, lies in the

nurturing of a tradition valorized by centuries-old practice, in the rejection of social and cultural experimentation, and especially in the non-acceptance of any supranational sources of legal authority. The concept of military neutrality that this country has opted for, and which is part of its political culture and national identity, in the conditions of the changed security paradigm in the post-Cold War period, has found itself facing expert demands to be re-examined and revised or changed on the basis of analysis. The vulnerability of the security and defense systems of almost all countries in the world, when they demonstrated their weakness and demonstrated a certain powerlessness in responding to various forms of threats aimed at national critical infrastructure in cyberspace, nullified the idea of developing independent protection mechanisms, with the traditional neutrality of the Swiss Confederation once again being put to the test.

Each strategy represents a multidimensional concept that inevitably encompasses all critical activities within the area to which it refers, whereby such a concept expressed through this form of a strategic document contributes to a sense of unity, direction and purpose in accordance with the given issue, while also acknowledging the necessary changes in the environment itself (Hax & Majluf, 1986: 6). Also known for the concept of total defense, which is included in the National Defense Strategy of this country, and which implies a comprehensive approach of the widest possible range of subjects of society for the purpose of military, civilian and other defense, Switzerland has implemented the same approach when designing a strategy for defense against cyber threats. An authentic approach of this type has resulted in the development of various institutional mechanisms for the defense of the country's critical infrastructure from cyber threats, with the subjects of that defense being mainly civilian structures. A well-established strategic framework in the field of cybersecurity has made this country relatively ready to respond to the largest number of security threats of this type; however, despite the fact that the center for collecting information on cyber threats at the national level should become an integral part of the country's Ministry of Defense, the absence of a military approach to this issue still remains the weakest element of the entire system. The lack of integration of military aspects into the general framework of cybersecurity of the Swiss Confederation results in inadequate affirmation of the subjects of protection against attacks of this type, because the examples presented here have shown that civilian structures cannot independently, without significant assistance from military structures in terms of both technology and personnel, develop all the necessary mechanisms for a complete response to threats from this spectrum. The persistence of the (political) will to take concrete steps towards a cyber-ready army in the near future, accompanied by appropriate resources, increases the likelihood that the Swiss Confederation will defend its reputation as a militarily neutral country ready to respond to all challenges, risks and security threats, no matter how demanding an independent response may be.

REFERENCE LIST

- Agius, C., & Devine, K. (2011). 'Neutrality: A really dead concept?' A reprise. *Cooperation and Conflict*, 46(3), 265-284.
- Baezner, M., & Cordey, S. (2019). *National cybersecurity strategies in comparison—Challenges for Switzerland*. Zurich: Center for Security Studies.
- Dahinden, M. (2021). *Swiss neutrality in the age of cyber warfare*. Geneva: ICT for peace foundation.
- Danspeckgruber, W. (2021). Armed neutrality: Its application and future. In *Securing Europe's Future* (pp. 242-279). Routledge.
- Fischer, D., Sauerwein, C., Werchan, M., & Stelzer, D. (2023). An Exploratory Study on the Use of Threat Intelligence Sharing Platforms in Germany, Austria and Switzerland. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (pp. 1-7).
- Hax, A. & Majluf, N. (1986). *Strategy and the Strategy Formation Process*. Cambridge: MIT Sloan School of Management.
- Huang, L., & Zhu, Q. (2019). Adaptive strategic cyber defense for advanced persistent threats in critical infrastructure networks. *ACM SIGMETRICS Performance Evaluation Review*, 46(2), 52-56.
- ISC2 Website, "ISC2 Research Reveals the Cybersecurity Profession Must Grow by 3.4 Mil to Close Workforce Gap", 20 April 2024. <https://www.isc2.org/Insights/2022/10/ISC2-Research-Reveals-the-Cybersecurity-Profession-Must-Grow-by-3-4-Mil-to-Close-Workforce-Gap>
- Jensen, E. T. (2011). Sovereignty and neutrality in cyber conflict. *Fordham International Law Journal*, 35(3), 815-841.
- Knežević, S., Cvetković, D., Mićović, M., Mitrović, A. & Milojević, S. (2021). Analysis of the Presence OF Criminal Offenses in the Field of the Shadow Economy in Serbia. *Lex Localis-Journal of Local Self-Government*, 19(1), 131-147.
- Kelsey, J. T. (2008). Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare. *Michigan law review*, 1(3), 1427-1451.
- Mićović, M. (2015). Karakteristike infrastrukturnih sistema. U V.M.Cvetković, M.Popović, T.Kesić, Ž.Nikač (ur), *Suprotstavljanje savremenom organizovanom kriminalu i terorizmu* (str. 375-385). Beograd: Kriminalističko-policijska akademija.
- Mićović, M. (2020). *Specifičnosti kritične infrastrukture u Republici Srbiji*. Beograd: Kriminalističko-policijski univerzitet.
- Müller, L. (2019). *Neutrality in world history*. Routledge.
- National Cyber Security Centre. (2023). *National Cyberstrategy*. Bern: The Federal Council. (file:///C:/Users/neman/Downloads/Nationale-Cyberstrategie-NCS-2023-04-13-EN.pdf)
- Neff, S. (2022). *The rights and duties of neutrals: A general history*. Manchester: Manchester University Press.

Putnik, N, Milošević, M. i Bošković, M. (2017). Strateško planiranje sajber odbrane – ka adekvatnijem pravnom okviru i novoj koncepciji procene rizika, izazova i pretnji. *Vojno delo*, 69(7), 174-185.

Steffen, B., & Patt, A. (2022). A historical turning point? Early evidence on how the Russia-Ukraine war changes public support for clean energy policies. *Energy Research & Social Science*, 91(2022), 1-10.

Vetschera, H. (1985). Neutrality and defense: Legal theory and military practice in the European neutrals' defense policies. *Defense Analysis*, 1(1), 51-64.

Hossam Nabil Elshenraky¹

THE MODERN SECURITY STRATEGIES IN CONFRONTING CYBER PHISHING ATTACKS

Abstract

One of the most serious cyber-attacks is phishing attack that relies on social engineering; it is considered one of the greatest security risks for institutions. Phishing methods vary between sending mass emails and text messages and attacks directed at sensitive user data. Phishing websites have an important role in attempting such crimes as well as imitation of sites to deceive victims and make them trust those fraudulent sites that the perpetrators use to phish their data. Various organizations that are exposed to phishing can defend against these attacks through email security solutions and Internet address filtering. However, the best solution is to train employees so that they do not become victims of phishing. To enhance their awareness of phishing methods, training courses are organized to detect phishing. The study adopted the approach of anticipating the phishing future in light of the technical development and predicting what it will be like and what the security methods are that can be confronted with it, as well as what the technical methods are that can be used to combat it in its various forms, then how the authorities in Dubai worked to find software and technical models that can be used to detect fraudulent links, methods and sites which work to phish victims over the Internet using various methods of social engineering. Also, what the models are prepared for training in detecting phishing methods and social engineering methods based on advanced technology and what the results are reached by various studies in the field of monitoring, detecting, and preventing phishing. Combating phishing requires security strategies developed by institutions that include training on detecting and monitoring phishing methods. Phishing is also the subject of in-depth scientific study from many parties. Scientific research developed many programs and models to prevent, monitor and detect phishing attempts, but training is important to raise the awareness of the employees and strong element in the defending against phishing. There are experiments and case studies conducted in the field of training employees and users to reduce falling victim to phishing, in addition to the presence of detection systems. Monitoring phishers and investigating phishing incidents is very useful in identifying prevailing phishing patterns and monitoring new patterns. New technical developments such as Meta verse and chat GPT produced new patterns and advanced and more complex phishing environments, which requires information security specialists and security personnel to monitor and understand its complex patterns and methods to combat it and reduce phishing.

Keywords: *phishing attacks, social engineering techniques, anti phishing campaign, vishing attacks.*

¹ Dubai police academy, UAE, habdelraouf@dubaipolice.ac.ae

INTRODUCTION

Phishing, which is a form of electronic attacks based on social engineering, represents the greatest security risk for organizations today. Phishing methods vary between sending mass emails and text messages to attacks directed at sensitive user data. Phishing websites have a serious role in successful phishing attack campaigns as well as imitation of sites to deceive victims and make them trust those fraudulent sites that the perpetrators use to phishing their data. Various organizations that are exposed to phishing can defend against these attacks through email security solutions and Internet address filtering, but the best solution is to train employees so that they do not become victims of phishing; business institutions allocate large budgets to train their employees so that they become aware of the various phishing methods and organize training courses for this according to well-prepared and planned programs to detect phishing and protect electronic communications. Social engineering methods are used in phishing attacks to achieve success, as the social engineer has become very hidden in its methods. After the success of these attacks, the troll accesses the information that was targeted by the attack by accessing the targeted accounts, which results in identity theft and financial losses (Jakobsson, 2006:59).

This is done by sending the victim a malicious file or phishing links. Therefore, users must be aware that phishing campaigns have become more professional, as spear phishing, business email phishing attacks, where the victims are targeted individuals or organizations. Once the user falls victim to phishing, action must be taken. To mitigate the negative effects resulting from this, various mechanisms are employed. In this study, we will discuss the description and analysis of phishing patterns, how to manage the processes of preventing and combating them, revealing their methods and the factors that affect them, how applied and theoretical scientific studies and research have analyzed these patterns of fraud, and what the models are that can be relied upon in monitoring and detecting phishing.

Aims:

- 1- Declare the dangers of phishing attacks and the importance of preventing them.
- 2 - Explain the new methods of security strategies to prevent and detect phishing attacks.
- 3 - Explore case study in higher education institute in implementing new security method to prevent phishing attacks.

Questionnaire:

- 1 - Dangers of phishing attacks;
- 2 - The importance of preventing phishing;
- 3 - What are raising awareness of phishing attacks techniques?
- 4 - How to investigate phishing attacks?
- 5 - What are the new techniques to prevent future phishing attacks?

Research methodology:

The scientific method is the descriptive and analytical method based on analyzing the results of a case study of experimenting with a training strategy on phishing patterns in higher education institutions.

This study aims to clarify the concept and mechanisms of phishing attacks.

1. Understand and analyze phishing attack types and methods.
2. Understand and anticipate phishing attacks considering technical development and emergence of unprecedented capabilities for perpetrators such as metaverses, which led to a radical change in the methods and environments of phishing, to find solutions to the new techniques of phishing.
3. Analyse studies to generate solutions to prevent phishing, train to combat phishing, and mechanisms to achieve it.
4. Understand mechanisms of prevention, monitoring and detection of phishing resulted from literatures.

DANGERS OF PHISHING ATTACKS

In the modern era of digitalization, when technology enables smooth communication and transactions, phishing risks are more significant than ever. Phishing is a sophisticated cyberattack technique used by hostile actors to trick victims into divulging personal information. It is a serious risk to people, companies, and even governments. Knowing the dangers of phishing is crucial for protecting against its sneaky effects, as hackers are always improving their methods and taking advantage of human weaknesses.

Phishing attacks are estimated to have cost businesses and individuals billions of dollars in losses because people have numerous personal social networking accounts that hold sensitive personal information such as private photos and vital information. These accounts also put people and their institutions' reputation at risk of being compromised by phishers. Additionally, with the start of the epidemic and the abrupt digital transformation of both governmental and private institutions' as well as individuals' personal, professional, and institutional activities, there has been an upsurge in phishing offenses, as witnessed and documented. One of the most notable of these innovations that exposed workers to more phishing attempts was the ability to work and learn remotely from home. Phishing awareness is important because, as statistics show, three US universities were the target of fraudulent ransomware attacks, which started with a phishing email. This underscores the significance of employee awareness and task performance regarding phishing to prevent unauthorized access to sensitive information (Moore, 2021:11).

The most effective defense against phishing risks for companies is awareness. As phishing awareness is a dynamic process that requires management, some organizations have used training efforts to raise people's understanding of phishing (Suganya, 2016:13).

Phishing campaigns are designed to teach staff members how to spot phishing emails and respond appropriately, thereby raising users' awareness of security and reducing their vulnerability to fake emails (Patil & Devale, 2016: 9).

Aleroud and Zhou suggest that the two primary methods for raising cybersecurity awareness are to train people and to utilize a phishing IQ test that mimics a phishing assault (Chatchalermpon & Daengsi, 2020: 10).

After multiple executions, Acquisti, Cranor, Hong, Blair, and Pham proposed embedded training to increase phishing awareness (Rahmad et al., 2020: 7).

Few studies have examined integrated phishing awareness campaigns that incorporate phishing attack simulations and embedded anti-phishing training. These studies rely on conditioning to understand the impact of campaigns on users, since phishing attacks awareness consider a process of learning that shapes people's attitudes and can be improved through rewards and penalties (Townsend, 2021: 6).

Studies have demonstrated that reinforcement can change an organism's attitude; that is, an organism's reinforced attitude tends to get stronger while its non-reinforced attitude gets weaker. In this regard, theories of conditioning are helpful because phishing awareness serves as a backup plan for reinforcement (Z.A. Wenet et al., 2019: 12).

Research has indicated that an organism's attitude can be altered by reinforcement; that is, an organism that receives reinforcement tends to have stronger attitudes while receiving less reinforcement tends to have weaker attitudes. Theories of conditioning are useful in this context since phishing awareness acts as a fallback for reinforcement (Bragg et al., 2019: 11).

To speed up learning and raise phishing awareness – which can be obtained gradually – the cybersecurity team in the Skinner case study sets up phishing awareness operations and training courses. Enhancing anti-phishing training among employees, using anti-phishing programs, must be dynamic and interactive, which can be achieved using various methods of training, especially scenario method, where a training scenario is developed based on targeting employees with phishing that simulates the truth and follows a mechanism (Kathrine, G.J.W., 2019: 14).

We can track how much a worker interacts with and reacts to phishing by keeping track of how many times a user clicks on links that are sent to them. Additional choices include teaching them virtually or through specialized workshops, which are efficient ways to teach staff members, and ensuring that the training materials are appropriate for the personnel (Downs, Holbrook and Cranor, 2006: 11).

When it comes to work management, the Board of Directors' management influence plays a significant role in distributing and putting into action awareness programs against phishing assaults. This helps to make the training relevant to the tasks completed by trainees and prioritizes them. High-level personnel are more vulnerable because it has been observed that they are unaware of spear phishing trends.

Technological solutions are also linked to prevention and awareness. Employees who receive training in phishing techniques are better equipped to recognize and report suspicious messages, remain warning, and take wise actions to confront it. Awareness areas ought to encourage trainees to utilize multi-level authentication and strong passwords in addition to providing techniques for detecting phishing mail.

These are instances of awareness campaigns as a component of phishing prevention:

a. Europol 2018 #Cyberfraud campaign: During Cybersecurity Month in Europe in 2018, the #Cyberfraud education campaign was initiated in collaboration with security agencies from both EU and non-EU member states as well as 24 banking unions. Awareness materials were presented in 27 languages and included information about common phishing scams and how to avoid them (Yeoh et al., 2021).

b. "Think before click": To help people better manage and resist financial scams, particularly banking scams, financial fraud Action UK launched this awareness campaign. The initiative is government-backed and run by financial services firms as well as UK payment industry institutions. The business and public sectors, communications service providers, security services, and others exhort people to consider the veracity of the information and data that is being distributed (Firman firmansyah, 2021).

c. European Union Phishing Initiative: A website that is backed by the EU and provides a means of reporting phishing attempts and identifying new patterns that hackers are using to reduce browser-related attacks. The trainer Phishing team creates collaboration between different sectors, unites stakeholders in the fight against phishing. Comprising approximately 2,200 members from diverse agencies, NGOs have reaped numerous benefits around information sharing and raising awareness of the techniques and risks associated with phishing (Jensen, 2017).

d. London Protocol: It is launched by the CASC to reduce phishing attacks with certificates and it is carried out voluntarily with the participation of certification authorities.

In the end, it can be said that awareness is the suitable way to defend against social engineering campaigns because of reducing risks and threats that could affect the pillars of the insurance plan for information systems, such as security chains and employees; awareness enhances users' understanding regarding securing their networks and increases the ability to identify phishing cyber criminals and report phishing activities that affecting personal and organization security (Naser et al., 2021).

THE IMPORTANCE OF PREVENTING PHISHING ATTACKS

Avoiding phishing attempts is crucial in the hyperconnected world of today, when digital transactions and communications are a part of everyday life. Phishing is a dangerous method that hackers employ to trick people into giving critical information. It seriously jeopardizes financial security, personal privacy, and organizational integrity.

Raising awareness of phishing attacks techniques

1. Methods of raising awareness of phishing attacks tricks

Researchers developed a method to raise awareness of the risks involved in phishing based on phishing emails and online games (Faivusovich, 2023: 14).

Other researchers also developed a phishing simulation game called “What Hack” and an analytical comparison with this game was made.

Also, others designed a game on smartphone application named “No Phish” to train employees to differentiate between real and fake addresses aimed at phishing them; they also proposed a strategy to combat phishing attacks and create a verifiable phishing training game.

As for the first group, they found that the gaming method is very effective in training employees to detect phishing.

Another researcher group also found that providing embedded training after an employee was attacked rather than sending same simulating phishing email is effective in training when employees realize that they are unable to recognize phishing emails. A phishing simulation with embedded training is an effective awareness experience, like a combination of notes and graphics about phishing used. Many studies revealed that training through interactive content is effective to enhance phishing security awareness, in line with attitude sciences.

A case study was conducted at a university in Australia (Chatchalermpun, 2020). It was about reducing number of employees who were deceived and phished by an e-mail, increasing the reports of phishing emails to enable security response team to reduce the loss and identifying vulnerable groups of phishing attacks.

Many employees ensured that results represented all levels of employees, from high rank management to workers and the total number of employees was 10,928. During the period of 6 months, 6 phishing awareness courses were organized, with 6 methods of phishing emails, with each course lasting one month.

According to the principle of attitude of science, a habit developed in 28 days; thus, the training course was scheduled once every month, the type of phishing attack simulation the trainee received via email depended on that month in which training on phishing attack began. All phishing emails contained codes that detected employees’ interactions with simulated phishing emails, such as replying, clicking on phishing links, or reporting if someone became victim of a phishing email; then the cyber security officers directed the employees to a video contained phishing content on the training page.

The training program also did not keep or store the trainees’ real passwords or any other data, even if trainees used them in the form fields the program was designed for; if trainees accessed phishing page prepared for training immediately after falling into training phishing trap, they would not fall into it (Patil & Devale, 2016: 9).

Phishing emails can be identified by the following:

- a. The names and addresses in the e-mail sender box are not the same.
- b. The presence of mistakes in the email, such spelling, grammar mistakes, or wrong spaces.
- c. E-mail pushing the receiver for immediate action.
- d. The link text does not match when the cursor passed between text and displayed links.

2. Raising the awareness of phishing and embedded framework of training

Embedded training frameworks offer a proactive and integrated approach to educating employees about phishing threats, empowering them to become the first line of defence against cyber-attacks.

By embracing these frameworks, organizations can cultivate an understanding of cybersecurity awareness and resilience in the face of evolving digital threats. Raising phishing attacks awareness and training framework build on operant conditioning rules to update the internal awareness about social engineering and phishing techniques; framework starts with everyone by receiving pushing emails to activate a link to an popup websites, which is considered an unsafe transaction; if the user responds insecurely to the fraudulent e-mails, opens the scam attachment, or neglects it, and user's transaction data are collected, that action directs users to "retrying login" page and then receiving "embedded training" on the web page enhancing their awareness of their attitude; such phishing mail is redirected to a web page containing phishing information, the web page contains videos on recognizing phishing methods, for example, when receiving e-mail, it includes link to the cybersecurity awareness website and a phishing awareness module. If user reports a phishing e-mail by Phishing Alerts, the employees will see "Congratulations, you have detected a phishing try through a simulation training campaign ", trainee will receive message from security team, that reported phishing e-mail is blacklisted, which reinforces trainee's secure attitude (A. F. AL-Otaibi & E. S Alsuwat, 2020).

Training data are recorded in the phishing simulation platform's database, which aims to understand the impact of phishing attacks and blended training, However, sensitive information used by trainees is not stored, while phishing awareness simulations and training content will be useful as a framework for the other stakeholders of the training program. Cyber security in planning phishing awareness programs is universal and can be easily applied in any organization; also, phishing simulation sessions can be carried out in an organized manner.

Clicks on phishing links and emails for all modules gradually decreased from starting point through the six training cycles and had the lowest click-through rate of all modules and click-through rates ranged from 0% to 4%; 16.33% of trainees in 16

incidents clicked on external links in phishing emails; after starting point, unsafe response in a module to phishing emails was 0% (Kathrine, G.J.W, 2019).

In the first phase, 33% of users performed risky actions, which is the highest level of sensitive data disclosure in the training course; one unit did not expose to any dangerous procedures and therefore the best risk disclosure to other units was not more than 20%. Fraud alert system had an overall upward trend from the beginning of the training program, while reporting phishing emails was the highest in the campaign, 8% of the 16 departments during the base reported phishing emails, and the number reached 35% at the end of the phishing awareness training, which was the highest average; units were best managed at the beginning of training, they had similar values of 17% and 18%, while they were the worst in the beginning for not reporting phishing messages.

3. Analysis of the results

In six training courses, 8,189 trainees were exposed to phishing attack simulations. As a group of people who regularly visit the university, the trainees enabled the trainers to assess the campaign's effect on a sample of people who were trained. Of the phishing emails they received, 8.3% were clicked by the trainees, 6.9% were clicked by visitors who had a university email, and neither regular employees nor visitors clicked on the remaining 6.6% of emails (Farheen, 2022: 63).

The majority of the 66 trainees (54.6%) who clicked on a simulated phishing email at least four times (ranging from 0 to 7) were temporary employees. This analysis concentrated on other groups that are not the core of cybersecurity training programs and that reported phishing mails. The results indicate that 137 out of 8,189 trainees (1.7%) said that they received phishing emails more than 6 times (range 0 to 7).

This indicates that haphazard attempts to train subgroups of trainees are ineffective, and that 100% of trainees must receive training each month to improve internal defenses against phishing cyber threats. This is a challenging task that, if left unattended, could result in security "holes" caused by employees who lack awareness of potential threats; there's a time when users will be greatly impacted by training sessions, as scammers can target those users and exploit them to obtain critical university data (Ansari, 2022:61).

Because of this, organizations need to make sure that users who are likely to be exposed to phishing due to their jobs receive enough consistent and gradual training to comprehend the most recent phishing techniques and pass simulated training. This training must also be unexpected in terms of its content, method, gradation, and scenarios. Establishing a continuous, phased training program can help employees become more aware of potential threats in between training sessions (Downs et al., 2006).

Part-time instructors run the risk of making mistakes because the circumstances surrounding phishing attacks are always changing. Continuous training initiatives to

guarantee that new hires are adequately onboarded and to emphasize that security is a serious problem 24/7 – not just checking a box to satisfy minimum requirements – mean that everyone learns how to handle threats and, since trolls won't give up, training should be gradually increased in difficulty and the level of scenarios and simulations should be raised to improve employee awareness.

To guarantee that forecasts are accurate, cybersecurity professionals must raise their understanding of typical phishing strategies during training. Predicting actual threats in this environment is a challenging task that necessitates ongoing monitoring of the impact of training.

Companies that train their personnel to detect phishing attacks must train them once or twice a month, since random or intermittent training might have negative effects, even though sudden instruction is beneficial in identifying phishing assaults. The first step in training a cybersecurity team can involve assessing user performance. This is because having information about employees' "starting point" and how they respond to threats can help identify threat awareness issues and figure out how to handle and reduce them. Reports should include real-time KPIs and business intelligence that flow to higher levels while protecting user privacy (Jakobsson & Myers, 2006).

Clear graphs and succinct information outlining significant changes should be included in reports. Ensuring that parties receive reports, summaries of training campaigns, and board reviews, will keep them informed about accomplishments and highlight the impact of the training program. Cybersecurity officials are aware that trainees react differently to attack vectors by tracking "click sequences," as doing so puts them at risk.

Keeping track of employee's performance is necessary for maintaining a list of click sequences. Data research is needed to understand how different employee groups respond to risks, including new hires, executive leadership, and long-time staff members.

The cybersecurity team of the organization ought to organize training sessions that revolve around simulations and scenarios, adopting a more unique approach to email management. Awareness techniques ought to encompass adjusted frequency, prompt reminders, tailored simulations, and educational materials that bolster cognizance of employee groups susceptible to phishing because of their job duties, all while upholding employees' privacy.

Training can start when employees are divided into groups based on criteria such as the scenario's degree of complexity. Personalized attitude-based training for future phishing attempts is essential, as is content adaptation to meet the unique demands of a given situation. Training materials may contain demands for data or passwords, messages from sources or senders that appear trustworthy, or information specific to the position of the employee. Employee defenses are strengthened by materials that adjust to individual employee responses and particular attack vectors, leveraging human capital to the institution's benefit (Sheng et al., 2007).

Users will probably not fall into the phishing trap twice, but the sequential click-bait method should have dynamic and personalized time intervals between training sessions to give employees a degree of risk through data-driven learning. Therefore, scenario training should be repeated for staff members so that trained trainees receive two training sessions per session for the high-risk group. This will increase their familiarity with the training material and motivate them to participate in the sessions.

Given the legal ramifications for email compliance standards, it is critical to customize cybersecurity and phishing training subjects to the corporate cultures of each employee. You can raise employee's knowledge of realistic simulations and stealth attacks while also increasing the possibility that they will believe the email simulation by referencing popular news, national holidays, and social media.

Organizations can achieve satisfactory results through the planning, management, and analysis of training courses when they use a machine learning-powered platform. In contrast to having to offer such content manually, which takes a long time, the solution gives the cybersecurity team data-driven solutions, which speeds up the process of building and assessing internal simulations. Employee satisfaction with security training also rises when simulations and the ensuing training material are perceived as valuable and relevant in comparison to haphazard or out-of-context training to identify sophisticated attacks. This reduces the capacity of phishers to trick employees with sophisticated attacks, further augmenting the program's relevance.

Long-term employee awareness of potential email attacks can be changed by the business, giving it a huge competitive advantage in any sector that significantly depends on digital communications (W. Wang et al., 2019).

Detecting phishing attacks

Phishing attack detection is a multifaceted task, with several techniques for identifying different types of assaults. Attacks are constantly evolving, therefore it is important to monitor, identify, and lessen their impact.

There are six techniques to identify and lessen phishing attacks, which rely on comprehending and evaluating phishing websites and recognizing phishing attacks by inferring how they are carried out. These techniques are as follows:

1. The potential for phishing

By leveraging reputation scores gleaned from a particular website or from an anti-phishing environment; adding untrustworthy URLs to the blacklist, or list of forbidden websites is how the blacklist approach is carried out.

2. The approach is based on fuzzy rules

The data and information mentioned in the algorithm are examined using an algorithm, and phishing sites are attempted to be located. This method, which has 27 features, has been used to evaluate the dangers of phishing websites. A unique model is then produced for location prediction via unstructured data exploration.

3. Machine learning approach

The machine can be equipped with a variety of algorithms. For instance, becoming knowledgeable about random forests, an integrated educational classification system that is useful in combating phishing attempts and aims to gather classroom data and information with support vector machines (SVM), which efficiently solves classification difficulties. The training and testing phases are the other two primary phases of machine learning. This implies that the work's predicted accuracy throughout the training phase is solely dependent on the knowledge gained. Predictive accuracy will drop in tandem with a decline in the amount of obtained information, whereas fairness accuracy will rise as the amount of acquired information increases.

4. Cantina-based approach in this type uses two terms

- a. Using frequency and inverse document frequency (TF-IDF), a retrieval algorithm for document classification and comparisons, phishing sites can be identified.
- b. Based on the distinctions between legitimate websites and phishing sites, which employ an image based on visual resemblance; this strategy divides webpages into blocked sections according to visible signals.

Additional metrics, such similarity mapping, block area, and other metrics are considered to determine the visual similarity between phishing and legitimate and fraudulent webpages.

5. Training in the detection of phishing using games

Playing an online game helps consumers learn effective ways to prevent phishing scams (Ping Yi et al., 2018: 13). This game was designed by a team of scientists, and through a user study in which participants were assessed and their capacity to recognize fraudulent websites was measured, the game's ability to teach players the methods to avoid phishing and how to detect them was evaluated. The participants who played the game were found to be more adept at minigame fraudulent websites both before and after they engaged in one of three 15-minute anti-phishing training activities (using the game, reading an educational program on combating phishing that was created based

on the game, or reading training materials found on the Internet). This can be accounted for by the fact that the game's interactive format and instructional message content make it a highly effective tool for spreading awareness about phishing. The game was created through an iterative design approach that employed paper and flash to experiment with various design options. A prototype was created after playtests and input on the lesson plan and presentation. It was then piloted and refined depending on user feedback and attitude, honing the game mechanics and messaging, and developing an appealing visual and aural style with eye-catching graphics and noises.

Investigating phishing attacks

1. Incident Detection and Analysis

The investigative journey into a phishing attack begins with the crucial step of incident detection and analysis. Security professionals must be adept at identifying potential phishing incidents, which may manifest as suspicious emails, reports from vigilant users, or anomalies detected by advanced threat detection systems.

Analysis of the incident involves understanding the scope of the attack, identifying potential victims, and assessing the methods employed by the attackers. This initial phase lays the foundation for a comprehensive investigation, guiding the allocation of resources and determining the appropriate response strategy.

2. Forensic Analysis of Phishing Artifacts

Digital forensics serves as a cornerstone in the investigation of phishing attacks. Security experts meticulously analyze phishing emails, malicious URLs, and compromised systems to extract valuable insights. This forensic analysis aims to unravel the intricacies of the attack, providing details about its origin, execution, and potential indicators of compromise. Forensic experts employ specialized tools and techniques to reconstruct the timeline of events, uncovering the tactics used by cybercriminals to obfuscate their activities. This level of scrutiny is essential for developing a thorough understanding of the attacks.

3. Tracing IP Addresses and Domains

In the digital realm, every interaction leaves a trail of breadcrumbs. Investigators trace these digital footprints, including IP addresses and domains associated with the phishing campaign. This process involves collaborating with Internet service providers (ISPs) and domain registrars to identify the infrastructure used by cybercriminals. Tracing IP addresses and domains not only provides insights into the technical aspects of

the attack but also facilitates the mapping of the attackers' infrastructure. This information becomes instrumental in building a case for legal action and further collaboration with law enforcement agencies.

4. Collaboration with Law Enforcement

Phishing attacks often transcend geographical boundaries, which requires collaboration between cybersecurity professionals and law enforcement agencies. Sharing information and intelligence with relevant authorities is crucial for initiating legal proceedings against the perpetrators. Collaboration involves providing law enforcement agencies with detailed reports, evidence gathered during the investigation, and any information that could aid in identifying and apprehending the attackers. This joint effort enhances the chances of bringing the perpetrators to justice while also contributing to the broader fight against cybercrime.

Preventing future phishing attacks

1. Educating and Empowering Users

Preventing future phishing attacks goes beyond technical solutions; it requires a proactive approach to user education and empowerment. Cybersecurity professionals must engage in ongoing awareness campaigns, educating users about the latest phishing tactics and best practices for recognizing and reporting suspicious activity. Empowering users involves training them to be vigilant, encouraging the adoption of secure communication practices and fostering a culture of cybersecurity within organizations. By arming individuals with the knowledge to identify and report potential threats, organizations can significantly enhance their overall resilience to phishing attacks.

Combating phishing assaults presents several difficulties for those doing so, including ongoing investigation and response. Reducing the effects of a phishing attack and handling it effectively are thought to be extremely difficult tasks requiring a wide range of competencies. Because of this, it needs to be handled in a planned way, with an analysis of its stages – particularly if phishing is multi-stage and successive – and knowledge of the best way to gather information that will enable investigators to identify the origin of the attacks, stop them, and apprehend those responsible.

Responders to phishing attacks concentrate on the significance of mitigating the effects of attacks to ensure business continuity, given the high rates of targeting of organizations given the current digital transformation. This is because absence of security systems and training in phishing prevention leads to phishing attempts not being reported to the relevant authorities.

Thus, the possibility of reporting is contingent upon the nature of the phishing attempt, the extent to which the brand name was used, and whether other brand names were used. When a company's real name is used improperly in phishing attacks, more thorough countermeasures are implemented, and reports to the appropriate authorities are made more frequently.

Organizations also lack a clear and frequent process for reporting suspicious activities to the attack response team or to security authorities, as the activity may be directed to helpdesk, or it may be sent to a monitored mailbox from which information flows greatly, and companies may not know how and when to report it to the police (Suganya, 2016).

2. Phishing incidents analysis

Fraud losses must have previously happened to respond to phishing incidents, and the business must have done a threat assessment beforehand, technical solutions come second.

A variety of well-established strategies, ranging from generic to commercial solutions, are generally available to address spear phishing assaults due to their frequency and the harm they pose to the greater cyber ecosystem. The two components of technical defense against phishing are as follows:

a. Programs and policies.

Information security teams establish policies that follow best practices and try to seal the holes that allow trolls to enter the organization. These policies determine the rules and procedures that control how staff members use data and databases stored in the cloud, as well as the rules and permission levels. Information security regulations seek to stop users from adopting risky behaviors. Disable unsupported macros. Implement two-factor and multi-factor authentication to make procedures apparent to clients, including correspondence via the company website. The kinds of files that are included as attachments in phishing emails should be the focus of attention.

Organizations must also establish and implement policies that prohibit the use of undesired, dubious, or hazardous file types. This is because many phishing emails include attachments. LNK files, archive files, and EXE files are all very suspicious in corporations. Reducing reaction time and minimizing possible losses can be aided by best practices in monitoring and internal incident response procedures. Moreover, it entails executing scripts on the web server to stop trolls from misusing photos when posing as reliable websites.

b. Set up a Sender Policy System (SPF) in DNS24 to filter mail from unregistered servers and verify SMTP servers.

Address filtering, which assists users and organizations in preventing email spoofing, is accomplished by protocols such as domain message authentication, reporting and matching.

c. Keep an eye out for odd account activity.

Several accounts place orders for items to be shipped to the same address, different transactions are carried out from the same IP address, and best practices for coding minimize the likelihood that phishers will take advantage of weakly secured websites by scanning the network for cross-site scripting vulnerabilities (XSS).

d. Make sure phishers can't fake a website with their own interface by using the TARGET_top29 directive.

3. Crisis management of phishing attacks

Warning of the attack and gathering data Here, you are made "alert" to a possible phishing attack, and the matter is investigated (K. Althobaiti et al., 2021), examining the phishing assault by closely examining email messages and their contents and determining the extent of the damage by following these procedures:

a. Parsing the email address, which will include the sender's name. Sending a phishing email. It's also critical to remember that just because an email server is physically located somewhere does not indicate that the troll is nearby. It might be situated somewhere other than the email server.

b. Email message analysis: At this point, the message's actual contents need to be closely scrutinized because there are a lot of telltale indicators that are hard to notice right away.

4. Domain link analysis

If the phishing email message contains a questionable link, the phishing site needs to be investigated and the location of the data released needs to be ascertained (this includes figuring out the web server's TCP/IP address). It is also necessary to assess the damage level. As instances of this, consider:

a. Compute the total number of workers who are impacted.

b. Find out what steps staff members have taken in response to phishing emails.

c. Were any attachments downloaded by them?

d. Did they enter their personal information on a phishing website?

e. Were workstations, servers, wireless gadgets, and network infrastructure impacted?

5. Keeping the attack's damage within limits

This phase, which involves reducing the harm brought on by phishing, is the most crucial since it encompasses the following:

Identifying the impacted IT infrastructure points will allow you to ascertain which employees are impacted, promptly update their usernames and passwords, modify the login credentials for system users; smartphones that are impacted are "remotely wiped," meaning that private data and information are removed.

Passwords and usernames are reset on new phones and an eye is kept on user accounts and information infrastructure systems to spot instances of abuse.

Carefully organizing the shutdown of systems to allow for a more thorough inquiry into what transpired, without interfering with the organization's regular business activities (R. Das, 2020).

Steer clear of hazards, identifying ways to prevent a similar cyberattack in the future comes as the last step after the damage has been limited and all impacted areas of the business have been addressed. The following needs to be considered by employing outside cybersecurity experts to carry out a thorough investigation of the security breach; they may offer suitable security remedies and carry out a penetration test to find security flaws.

Make sure that a regular schedule is maintained for updating online browsers, installing software updates on servers, and using the most recent versions of anti-malware, anti-phishing, and anti-spyware programs.

When a phisher hacks login credential to assess the information infrastructure is impacted after individuals are impacted initially, it is important to emphasize staff awareness. It necessitates the hold training sessions on a regular basis, teach staff members how to spot phishing emails by having them look out for phony sender names, sender domains, and misspellings in the email's subject line or body; assess if a link is harmful by outlining the steps to go through the link in question to check if the domain matches what is being shown (J.A. Chaudhry, 2016: 10).

If they diverge, the link is harmful; they should get in touch with a known individual if they receive an unusual email or attachment to make sure they sent it. If not, the message needs to be deleted right once and forwarded to information security professionals.

Encourage staff members to trust their gut feelings and to report any suspicious emails, explain how to verify the legitimacy of websites and if the URL address bar displays "HTTPS", never click on a message that comes in on your work device (A. Ali, 2015: 30).

Employees in information security are required to occasionally send out phishing emails as a test of their awareness, requesting that the information security officer becomes knowledgeable about the most recent phishing tactics.

All servers need to have anti-phishing toolbars loaded, since these programs check visited websites for similarities with databases of well-known phishing sites. Testing routers, firewalls, and network penetration devices to update the network infrastruc-

ture. Determine which controls are ineffective and take action to replace them or make necessary corrections.

Establish a hotline that workers can use to get in touch with information security personnel immediately if they come across a phishing email (Dinna N.M.N. et al., 2007: 586).

CONCLUSION

1. There are many types of phishing, the most dangerous of which is based on social engineering methods. Combating phishing requires security strategies developed by institutions that include training on detecting and monitoring phishing methods.

2. Phishing is the subject of in-depth scientific study from many practical research bodies. Many programs and models have been developed to prevent, monitor, and detect phishing attempts, but training and awareness of employees remain the most important and strongest elements in the defense system against phishing.

3. There are many experiments and case studies that have been conducted in the field of training employees and users to reduce falling victim to phishing, in addition to the existence of systems to detect and monitor phishers and investigate phishing incidents, which are very useful in identifying prevailing phishing patterns and monitoring new patterns.

4. New technical developments, such as Meta verse and GPT chat, have produced new patterns and more sophisticated and complex environments for phishing, which requires information security specialists and specialized security personnel to monitor them and understand their complex patterns and methods to combat them and limit phishing.

5. The Emirate of Dubai has specified a model on its website through which phishing attempts are identified, reported and their patterns are determined. It is a free service available on its website and mentioned in the text of the research.

Recommendations

1. We believe that an integrated strategy to prevent fraudulent response should be developed, and its training will be binding on all government agencies and the private sector that deal with sensitive components of the state's infrastructure, and that employees who are appointed to jobs that deal with sensitive data of individuals and institutions should take it. After taking the prescribed courses, each according to the level of the job and the extent of access to the data, to ensure the availability of awareness among employees dealing with sensitive data, the extent of awareness is tested in a sudden and unannounced manner according to a secret plan to ensure the readiness of those dealing with the state's sensitive information systems to detect and monitor phishing.

2. A specialized study should be prepared, and a national working group should be allocated that uses foreign expertise with experience in the field of information security to develop an integrated system for cybersecurity and monitor phishing activities, and a unit should be allocated in the Federal Communications Commission, assisted by electronic investigation officials, specialized in combating phishing activities and preparing studies and research on the matter. The developments occur in phishing patterns; because of the danger this crime poses to cyber trust and thus the country's digital economy, considering the accelerating digital transformation in all fields, it requires the presence of mechanisms capable of deterring crime, perhaps the most dangerous of which is phishing; it undermines efforts for economic growth and the protection of confidential and sensitive data in government institutions and the private sector.

REFERENCE LIST

10 Best Practices for an Effective Phishing Simulation Program, The Phishing Simulations Playbook, <https://cybeready.com/wp-content/uploads/PhishingSimulation-sPlaybook.pdf>.

A.S. Hovan George, Maschio Fernando, Dr. A.Shaji George, Dr.T.Baskar, Digvijay Pandey, Metaverse: The Next Stage of Human Culture and the Internet, *International Journal of Advanced Research Trends in Engineering and Technology* (IJARTET) Vol. 8, Issue 12, December 2021, <https://www.bing.com/ck/a?!&&p=bc187f86ecdd85acJmlt-dHM9MTY4OTAzMzYwMCZpZ3VpZD0xYjYxZTJmOS1kYTY0LTZkZjAtMzdlMy1mMWZmZGJiYzZjNjMmaW5zaWQ9NTMyOA&ptn=3&hsh=3&fclid=1b61e2f9-da64-6df0-37e3-f1ffdbbc6c63&u=a1aHR0cHM6Ly93d3cucmVzZWFiY2hnYXR-llm5ldC9wdWJsaWNhdGlvbi8zNTczNTQ5MzJfTWV0YXZlcnNlX1RoZV9OZXh0X1N0YWdlIX29mX0h1bWFuX0N1bHR1cmVfYjYw5kX3RoZV9JbnRlcm5ldA&ntb=1>

Abdul Ali, Social Engineering: Phishing latest and future techniques, Conference Paper April 2015, https://www.researchgate.net/publication/274194484_Social_Engineering_Phishing_latest_and_future_techniques?enrichId=rgreq-7d1ea0ebb698f8ea52ec3b44cc5a81bc-XXX&enrichSource=Y292ZXJQYWdlOzI3NDE5NDQ4NDtBU-zoyMTI0NDQyMjQ5ODcxMzZAMTQyNzY2MjA1ODc5Mw%3D%3D&el=1_x_2&_esc=publicationCoverPdf

Abeer F. AL-Otaibi & Emad S Alsuwat, College of Computers and Information Technology, Taif University, Saudi Arabia, study on social engineering attacks: phishing attack, *International Journal of Recent Advances in Multidisciplinary Research* Vol. 07, Issue 11, pp. 6374-6380, November 2020, https://www.researchgate.net/publication/348606991_A_STUDY_ON_SOCIAL_ENGINEERING_ATTACKS_PHISHING_ATTACK?enrichId=rgreq-798fb7d57b7e01fe244c0ca32af34f29-XXX&enrichSource=Y292ZXJQYWdlOzI3NDE5NDQ4NDtBU-zoyMTI0NDQyMjQ5ODcxMzZAMTQyNzY2MjA1ODc5Mw%3D%3D&el=1_x_2&_esc=publicationCoverPdf

TYxMTA4NDU1OTMwNQ%3D%3D&el=1_x_2&_esc=publicationCoverPdf

Abeer F. AL-Otaibi and Emad S Alsuwa, A study on social engineering attacks: phishing attack, College of Computers and Information Technology, Taif University, Saudi Arabia, *International Journal of Recent Advances in Multidisciplinary Research* Vol. 07, Issue 11, November 2020.

Affan Yasin, Rubia Fatima, Lin Liu, Jianmin Wanga, Raian Ali, Ziqi Wei, Counteracting social engineering attacks, *Journal of Computer Fraud & Security*, October 2021, https://www.researchgate.net/publication/355585293_Counteracting_social_engineering_attacks?enrichId=rgreq-69716957fe9cc46a2e1a3703964f7be1-XXX&enrichSource=Y292ZXJQYWdlOzM1NTU4NTI5MztBUzoxMDgzMTk2OTMwMjZyYQDE2MzUyNjU2ODE4NDY%3D&el=1_x_2&_esc=publicationCoverPdf

Ahmed Mohamed, *Phishing, and social engineering techniques*, April 18, 2013, <https://resources.infosecinstitute.com/topic/phishing-and-social-engineering-techniques/>

Alex Faivusovich, *Fraud Fighters Manual for Fintech, Crypto, and Neobanks*, 2023, pp:123-125, <https://www.unit21.ai/resources/fraud-fighters-manual>

Ammar Naser, Mahmoud Jazzar, Derar Eleyan, Amna Eleyan, Social Engineering Attacks: A Phishing Case Simulation, *International Journal of Scientific & Technology Research*, Volume 10, Issue 03, March 2021, www.ijstr.org

Ammar Naser, Mahmoud Jazzar, Derar Eleyan, Amna Eleyan, Social Engineering Attacks: A Phishing Case Simulation, *International Journal of Scientific & Technology Research*, Volume 10, Issue 03, March 2021. https://www.researchgate.net/publication/350710068_Social_Engineering_Attacks_A_Phishing_Case_Simulation?enrichId=rgreq-6a99e2db5d0d89405c98a75f0ca3992a-XXX&enrichSource=Y292ZXJQYWdlOzM1MDcxMDA2ODtBUzoxMDEwMDY5Mjk4NzUzNTM2QDE2MTc4MzA2OTUwOTI%3D&el=1_x_2&_esc=publicationCoverPdf

Anjum N. Shaikh& others, A Literature Review on Phishing Crime, *Prevention Review, and Investigation of Gaps*, Conference: 2016, *10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*.

ASEAN Cybersecurity Cooperation Strategy (2021 – 2025), https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

ASEAN Cyberthreat Assessment 2021, *Key Cyberthreat Trends Outlook From, The Asean Cybercrime Operations Desk*, pp:15-18,2021, <https://www.interpol.int/en/content/download/16106/file/ASEAN>

Ayesha Arshad, Attique Ur Rehman, Sabeen Javaid, Tahir Muhammad Ali, Javed Anjum Sheikh, Muhammad Azeem, A Systematic Literature Review on Phishing and Anti-Phishing Techniques, *Pakistan Journal of Engineering and Technology, PakJET Multidisciplinary & Peer Reviewed* Volume: 04, Number: 01, Year: 2021, <https://arxiv.org/ftp/arxiv/papers/2104/2104.01255.pdf>

Biju Issac, Raymond Chiong and Seibu Mary Jacob, Analysis of Phishing Attacks and Countermeasures, Conference Paper, January 2006, https://www.researchgate.net/publication/235947501_Analysis_of_Phishing_Attacks_and_Countermeasures?enrichId=rgreq-9276f977873eb470a08aa0b68079de46-XXX&enrichSource=Y292ZXJQYWdlOzIzNTk0NzUwMTtBUzo5OTQxMzgyNTQyNTQyNkAxNDAwNzEzNTExNTQz&el=1_x_2&_esc=publicationCoverPdf

Caitlin Jones, *50 Phishing Stats You Should Know In 2023*, <https://expertinsights.com/insights/50-phishing-stats-you-should-know/>

ChatGPT, *The impact of Large Language Models on Law Enforcement, Europol Public Information*, 2023, <https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf>

Cyber considerations for the Metaverse, KPMG, 2023 <https://assets.kpmg.com/content/dam/kpmg/ch/pdf/cyber-considerations-metaverse-ch.pdf>

Cyber crime, COVID 19 impact, INTERPOL report 2020, Lyon Francep:8, file:///C:/Users/Admin/Downloads/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

Dinna N. M. N., Leau Y. B., Habeeb S. A. H., and Yanti A. S., Managing Legal, Consumers and Commerce Risks in Phishing, Open Science Index, World Academy of Science, Engineering and Technology, *International Journal of Economics and Management Engineering*, Vol:1, No:11, 2007, pp:586-588, https://www.researchgate.net/publication/238683028_Managing_Legal_Consumers_and_Commerce_Risks_in_Phishing?enrichId=rgreq-50426eb6e29e99f5b0242bfd1933cd2b-XXX&enrichSource=Y292ZXJQYWdlOzIzODY4MzAyODtBUzo4OTA2MTAxMzk1Mzc0MDhAMTU4OTM0OTQxMjc2OQ%3D%3D&el=1_x_2&_esc=publicationCoverPdf

Downs, J., M. Holbrook and L. Cranor. 2006. Decision strategies and susceptibility to phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania, July 12 - 14, 2006). SOUPS '06, vol. 149. ACM Press, New York, NY, 79-90. DOI= <http://doi.acm.org/10.1145/1143120.1143131>

Elmer EH Lastdrager, *Achieving a consensual definition of phishing based on a systematic review of the literature*, 2014 Lastdrager; licensee Springer, <http://www.crimesciencejournal.com/content/3/1/9>

F Rahmad , Y Suryanto , K Ramli, Performance Comparison of Anti-Spam Technology Using Confusion Matrix Classification, IOP Conference Series: *Materials Science and Engineering*, *Materials Science and Engineering* 879 (2020) 012076, <https://iopscience.iop.org/article/10.1088/1757-899X/879/1/012076>

Firman firmansyah, Exposing generational and gender gap in phishing awareness among young adults: A survey experiment, VII international conference *Safety problems of civil engineering critical infrastructures* (SPCECI2021), <https://www.acad->

emia.edu/99615520/Exposing_generational_and_gender_gap_in_phishing_awareness_among_young_adults_A_survey_experiment

Global landscape on COVID-19 cyberthreat, Interpol, 2020, p:2, file:///C:/Users/Admin/Downloads/Global%20landscape%20on%20COVID-19%20cyberthreat.pdf

Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R. C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens, *Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic*, 2020, https://penta.ch/solutions/it-risk-solutions/cyber-security-awareness-training/?utm_term=cyber%20awareness&utm_campaign=CTX-DXB-ITRisk&utm_source=bing&utm_medium=ppc&hsa_acc=4309067005&hsa_cam=15523479340&hsa_grp=1185274557785084&hsa_ad=&hsa_src=o&hsa_tgt=kwd-74079863511700:loc-218&hsa_kw=cyber%20awareness&hsa_mt=b&hsa_net=ad-words&hsa_ver=3&mclid=4d3687b2b506177fee2be31e0c34a303

Hossein Abroshan (&), Jan Devos, Geert Poels, and Eric Laermans, *Phishing Attacks Root Causes*, Springer International Publishing AG, part of Springer Nature 2018 N. Cuppens et al. (Eds.): Crisis 2017, LNCS 10694,2018. https://doi.org/10.1007/978-3-319-76687-4_13

<https://resources.infosecinstitute.com/topic/the-phishing-response-playbook/>

Huber, M., Kowalski, S., Nohlberg, M., and Tjoa, S. (2009). "Towards automating social engineering using social networking sites," in 2009 *International conference on computational science and engineering*, Vancouver, BC, August 29–31, 2009 (IEEE, 117–124. doi:10.1109/CSE.2009.205

Ike Vayansky and Sathish Kumar, *Phishing – challenges and solutions*, 2018, pp:2-4, https://www.researchgate.net/publication/322823383_Phishing_-_challenges_and_solutions?enrichId=rgreq-767e9f87bbb48d3c1e1f6e697c258175-XXX&enrichSource=Y292ZXJQYWdlOzMyMjgyMzM4MztBUzo2MTQxODM3MjA3MzA2ND-dAMTUyMzQ0NDIxODMyMA%3D%3D&el=1_x_2&_esc=publicationCoverPdf

Internet Organized Crime Threat Assessment (IOCTA) 2021, European Union Agency for Law Enforcement Cooperation, Publications Office of the European Union, https://ec.europa.eu/eusurvey/runner/eus_strategic_reports

Internet organized crimes threat assessment, Europol, 2020.

Jakobsson, M., and Myers, S., Eds. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley-Interscience, 2006,pp: <https://www.semanticscholar.org/paper/Phishing-and-Countermeasures%3A-Understanding-the-of-Jakobsson-Myers/7a54d9de33e784128248dbf2e72160250d321aa1>

Junaid Ahsenali Chaudhry, Shafique Ahmad Chaudhry, Robert G. Rittenhouse, *Phishing Attacks and Defenses*, *International Journal of Security, and Its Applications* Vol. 10, No. 1 (2016), <http://dx.doi.org/10.14257/ijisia.2016.10.1.23>

Junaid Ahsenali Chaudhry, Shafique Ahmad Chaudhry, Robert G. Rittenhouse, Phishing Attacks and Defenses, *International Journal of Security and Its Applications*, V ol. 10, No. 1 (2016), pp.247-256, <http://dx.doi.org/10.14257/ijasia.2016.10.1.23>

Kaouthar Chetoui, Birom Bah a, Abderrahim Ouali Alami a, Ayoub Bahnasseb, Overview of Social Engineering Attacks on Social Networks, *The second International Workshop of Innovation and Technologies (IWIT 2021)* November 1-4, 2021, Leuven, Belgium, https://www.researchgate.net/publication/358132130_Overview_of_Social_Engineering_Attacks_on_Social_Networks?enrichId=rgreq-547cd80a603d9313ce2b7713ac4be9d6-XXX&enrichSource=Y292ZXJQYWdlOzMlODEzMjEzMDtBUzozMTE2NjI2NTg1OTU2MzUyQDE2NDMyMzU5MzIwNjE%3D&el=1_x_2&_esc=publicationCoverPdf

Kathrine, G.J.W., et al. Variants of phishing attacks and their detection techniques. in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. 2019. IEEE, <https://ieeexplore.ieee.org/xpl/conhome/8851338/proceeding>

Kevin Townsend, *Europol on Methodology Behind Successful Spear Phishing Attacks*, <https://www.securityweek.com/europol-methodology-behind-successful-spear-phishing-attacks/>

Kholoud Althobaiti, Adam D. G. Jenkins, University of Edinburgh, Kami Vaniea, A Case Study of Phishing Incident Response in an Educational Organization, *Proc. ACM Hum.-Comput. Interact.*, Vol. 5, No. CSCW2, Article 338. Publication date: October 2021., pp:3-6, <https://groups.inf.ed.ac.uk/tulips/papers/althobaiti2021csw.pdf>

Lindiwe T. Hove, Strategies Used to Mitigate Social Engineering Attacks, Walden University, *Scholar Works, College of Management & Technology*, 2020

M. Jakobsson and S. Myers. Wiley-Inter science, In *Phishing and Countermeasures*, eds, 2007,

Matthew L. Jensen, Alexandra Durcikova, Ryan T. Wright, Combating Phishing Attacks: A Knowledge Management Approach, *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017, pp: 4288-2489, <http://hdl.handle.net/10125/41681>

Matthew NO Sadiku, Adebowale E Shadare, Sarhan M Musa, Social Engineering: An Introduction, *Journal of Scientific and Engineering Research*, 2016, 3(3):64-66, https://www.researchgate.net/publication/308315268_Social_Engineering_An_Introduccion?enrichId=rgreq-009fbcba47004f896dc77ba3398904d-XXX&enrichSource=Y292ZXJQYWdlOzMwODMxNTI2ODtBUzo0MDgxNzA4MDQ1OTY3MzZAMTQ3NDMyNjIxMTIwNA%3D%3D&el=1_x_2&_esc=publicationCoverPdf

Meraj Farheen Ansari, Pawan Kumar Sharma, Bibhu Dash, Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training, Vol. 3: Iss. 3, Article 6., 2022, pp:61-63, <https://www.interscience.in/ijssan>

Mike Moore, *Don't open that PDF email attachment - it could well be malware*, published April 08, 2021, <https://www.techradar.com/news/dont-open-that-pdf-email-attachment-it-could-well-be-malware>

Muhammet Baykara, Zahit Ziya Gürel, *Detection of phishing attacks*, 2018, pp:2-4, https://www.researchgate.net/publication/324999540_Detection_of_phishing_attacks-enrichId=rgreq-b470bb2fcf352150e80d90a579a5e107-XXX&enrichSource=Y292ZXJQYWdlOzMyNDk5OTU0MDtBUzo2NTY5NDcwMDcyMDk0NzNAMTUzMzYzOTc4MDEzMw%3D%3D&el=1_x_2&_esc=publicationCoverPdf

P.Kalaharshaa,b , B. M. Mehtrea, *Detecting Phishing Sites - An Overview*, 2021, pp:2-6, <https://arxiv.org/pdf/2103.12739.pdf>

Pandemic profiteering how criminals exploit the COVID-19 crisis, Europol, March 2020, pp:6-8, <https://www.europol.europa.eu/publications-events/publications/pandemic-profiteering-how-criminals-exploit-covid-19-crisis>

Phishing Activity Trends Report, 2nd Quarter 2020, Activity April-June 2020, Published 27 August 2020, https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf

Phishing Simulation Testing, *Deliver the Right Training at the Right Time for the Right Person*, <https://20641927.fs1.hubspotusercontent-na1.net/hubfs/20641927/Solution%20Briefs/Phishing%20Simulation%20%26%20Training.pdf>

Ping Yi, Yuxiang Guan, Futai Zou, Yao Yao, Wei Wang, Ting Zhu, *Web Phishing Detection Using a Deep Learning Framework*, *Research Article, Open Access*, Volume 2018, pp:2-3, <https://doi.org/10.1155/2018/4678746>

Pratik Patil, Prof. P.R. Devale, *A Literature Survey of Phishing Attack Technique*, *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 5, Issue 4, April 2016, pp:195-197, <https://ieeexplore.ieee.org/document/7813778#:~:text=A%20literature%20survey%20on%20social%20engineering%20attacks:%20Phishing,fool%20an%20online%20user%20into%20elicit%20personal%20Information>

Rasha Salah El-Din, Paul Cairns & John Clark, *Mobile Users' Strategies for Managing Phishing Attacks*, *Journal of Management and Strategy* Vol. 5, No. 2; 2014, pp:75-79, https://www-users.york.ac.uk/~pc530/pubs/Rasha_JMS2014.pdf

Ravi Das, *The phishing response playbook*, 2018, infosec,

Ravi Das, *The phishing response playbook*, <https://resources.infosecinstitute.com/topic/the-phishing-response-playbook/>

Sayak Saha Roy, Krishna Vamsi Naragam, Shirin Nilizadeh, *Generating Phishing Attacks using ChatGPT*, 2023, pp:1-5, <https://arxiv.org/pdf/2305.05133.pdf>

Social engineering handbook How to Take the Right Action, 2021, https://www.eset.com/fileadmin/ESET/INT/Landing/2021/Project_progress/ESET-Social_engineering_handbook.pdf

Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, Elizabeth Nunge, *Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish*, Conference Paper· July 2007, pp:2-5, https://www.researchgate.net/publication/221166422_Anti-Phishing_Phil_The_Design_and_Evaluation_of_a_Game_That_Teaches_People_Not_to_Fall_for_Phish?enrichId=rgreq-99c91b4850edec184f32c9bccdd80bca-XXX&enrichSource=Y292ZXJQYWdlOzIyMTE2NjQyMjBUzoxMTQzMTE4MTE5NTc5NTM3MUAXNjc1MTAyMTA3NzAy&el=1_x_2&_esc=publicationCoverPdf

Surachai Chatchalermpon, Therdpong Daengsi, improving cybersecurity awareness using phishing attack Simulation, *Annual Conference on Computer Science and Engineering Technology (AC2SET) 2020*, <https://iopscience.iop.org/article/10.1088/1757-899X/1088/1/012015>

Surachai Chatchalermpon1, Therdpong Daengsi, Improving cybersecurity awareness using phishing attack simulation, *Annual Conference on Computer Science and Engineering Technology (AC2SET) 2020*, pp:1-3, <https://iopscience.iop.org/article/10.1088/1757-899X/1088/1/012015>

Takashi Koide, Naoki Fukushi, Hiroki Nakano, Daiki Chiba, Detecting Phishing Sites Using ChatGPT,2023, <https://arxiv.org/pdf/2306.05816.pdf>

Terry Egharevba, *Phishing Attack- A Challenge in Cybersecurity*, January 2022, IEEE, https://www.researchgate.net/publication/357826193_Phishing_Attack-A_Challenge_in_Cybersecurity?enrichId=rgreq-a0085ddb103191f6ad57662d53392715-XXX&enrichSource=Y292ZXJQYWdlOzM1NzgyNjE5MztBUzoxMTEyMDY2MjM2NjUzNTcxQDE2NDIxNDg2NjA0Mjc%3D&el=1_x_2&_esc=publicationCoverPdf

The escalation of digital fraud: global impact of the coronavirus, October 2020, javelin, <https://www.sas.com/en/whitepapers/escalation-of-digital-fraud-111830.html>

Understanding phishing techniques, December 2019, <https://resources.infocseinstitute.com/category/enterprise/phishing/phishing-as-a-risk-damages-from-phishing/reputational-damages/>

V. Suganya, A Review on Phishing Attacks and Various Anti Phishing Techniques, *International Journal of Computer Applications* (0975 – 8887), Volume 139 – No.1, April 2016, pp:20-22, <https://www.ijcaonline.org/research/volume139/number1/suganya-2016-ijca-909084.pdf>

Vaishnavi Bhavsar, Aditya Kadlak, Shabnam Sharma, Study on Phishing Attacks, *International Journal of Computer Applications* (0975 – 8887), Volume 182 – No. 33, December 2018, https://www.researchgate.net/publication/329716781_Study_on_Phishing_Attacks?enrichId=rgreq-941de64f16f41b7041fcc00ed7ad655d-XXX&enrichSource=Y292ZXJQYWdlOzMyOTcxNjc4MTtBUzo5MDE2NDY0ODgwNDM1MjBAMTU5MzQxMTE5NDY2Nw%3D%3D&el=1_x_2&_esc=publicationCoverPdf

Vanessa Gomes, Joaquim Reis, Bráulio Alturas, *Social Engineering and the Dangers of Phishing*, Conference Paper June 2020, https://www.researchgate.net/publication/342965568_Social_Engineering_and_the_Dangers_of_Phishing?enrichId=rgreq-aa5124c4af9c3d845a06cdb8deb60d13-XXX&enrichSource=Y292ZXJQYWdlOzM0Mjk2NTU2ODtBUzoxMTQ3NTk4Njg5ODQxMTUyQDE2NTA2MjAyNTcwMDM%3D&el=1_x_2&_esc=publicationCoverPdf

Weiping Wang, Feng Zhang, Xi Luo, Shigeng Zhang, PDRCNN: Precise Phishing Detection with Recurrent Convolutional Neural Networks, *Security and Communication Networks*, Volume 2019, Article ID 2595794, pp:3-6, <https://doi.org/10.1155/2019/2595794>

Weiping Wang, Feng Zhang, Xi Luo, and Shigeng Zhang, DRCNN: Precise Phishing Detection with Recurrent Convolutional Neural Networks, *Research Article, Open Access*, Volume 2019, Article ID 2595794, pp:10-11, <https://doi.org/10.1155/2019/2595794>

What Is Phishing, Education guide, Fortinet, 2019, <https://www.fortinet.com/content/dam/fortinet/assets/education/eg-guide-on-phishing.pdf>

What Is Phishing, Education guide, Fortinet, <https://www.fortinet.com/content/dam/fortinet/assets/education/eg-guide-on-phishing.pdf>

William Yeoh a, He Huang, Wang-Sheng Leeb, Fadi Al Jafaria, and Rachel Manssona, Simulated Phishing Attack and Embedded Training Campaign, *Journal of computer information systems*, 2021 International Association for Computer Information Systems, https://www.researchgate.net/publication/354231308_Simulated_Phishing_Attack_and_Embedded_Training_Campaign?enrichId=rgreq-66191ca14d5bae0fce1f59f615b3b7e-XXX&enrichSource=Y292ZXJQYWdlOzM1NDIzMTMwODtBUzoxMDg2MjEwNjM4Mzg1MTUyQDE2MzU5ODQyMDUwNjM%3D&el=1_x_2&_esc=publicationCoverPdf

William Yeoh, He Huang, Wang-Sheng Lee, Fadi Al Jafari & Rachel Mansson, Simulated Phishing Attack and Embedded Training Campaign, *Journal of Computer Information Systems*, 2021, <https://doi.org/10.1080/08874417.2021.191994>

Yohann Sillam and Daniel Alima, “The Turkish Rat” Evolved Adwind in a Massive Ongoing Phishing Campaign, February 17, 2020, <https://research.checkpoint.com/2020/the-turkish-rat-distributes-evolved-adwind-in-a-massive-ongoing-phishing-campaign/>

Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf and Imtiaz Khan, Phishing Attacks: A Recent Comprehensive Study and a New Anatomy, *Frontiers in Computer Science* March 2021, Volume 3, Doi: 10.3389/fcomp.2021.563060, www.frontiersin.org

Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, Erik Andersen, What. Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game, *CHI 2019*, May 4–9, 2019, Glasgow, Scotland, UK, paper 108, https://www.researchgate.net/publication/332745435_WhatHack_Engaging_Anti-Phishing_Training_Through_a_Role-play

ing_Phishing_Simulation_Game?enrichId=rgreq-3df63695d15b8b18a2e3c580368f92d0-XXX&enrichSource=Y292ZXJQYWdlOzMzMjc0NTQzNTtBUzo4OTYyMDAyNzg1NDg0ODIAMTU5MDY4MjIwNTQxNQ%3D%3D&el=1_x_2&_esc=publicationCoverPdf

Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, Erik Andersen, What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game, *CHI* 2019, May 4–9, 2019, Glasgow, Scotland, UK, file:///C:/Users/Admin/Downloads/WhatHack_Engaging_Anti-Phishing_Training_Through_a.pdf

*Gordana Mišev¹
Andjelija Djukić²
Miloš Tošić³*

CHALLENGES OF MILITARY NEUTRALITY IN THE CONTEXT OF CONTEMPORARY GEOPOLITICAL RELATIONS IN EUROPE⁴

Abstract

In a security environment where the biggest security threats include a wide range of military and non-military threats, no country can rely only on its own forces. The development trend of multilateral relations has a significant impact on the creation of the security policy of states. However, there is no consensus of global power centers on the direction of building a common global peace policy. The increasing confrontation of major powers (USA-RF), with the tendency to increase the number of influential states (China, Brazil, India) announces even more complex international relations. The war in Ukraine influenced Sweden and Finland to abandon their military neutrality status, while other European countries, including Austria and Switzerland, did not change the direction of their security policy. The Republic of Serbia with its unresolved internal issues, above all the status of AP of Kosovo and Metohija, is facing serious security challenges and the question arises whether military neutrality is the appropriate political direction for the protection of the national interest. Analyzing contemporary security threats and changes in geopolitical relations, it was concluded that military neutrality is the most adequate framework for creating the foreign and defense policy of the Republic of Serbia.

Keywords: *military neutrality, security, spheres of influence, global power centers, Europe.*

INTRODUCTION

Modern security challenges, risks and threats have become complex, unpredictable and transnational. The clear boundary between military and non-military threats has been erased, i.e. threats to security have both military and economic, political, social, environmental and technological dimensions. Security assessment therefore includes a

¹ Faculty of Diplomacy and Security, Belgrade, Serbia, gmisev77@gmail.com

² Institute for Strategic Research, University of Defence, Belgrade, Serbia

³ Faculty of Business and Law, MB University, Belgrade, Serbia

⁴ The paper was created as part of the scientific research project: "Challenges of military neutrality and political identities in contemporary geopolitical challenges" in partnership with the Faculty of Diplomacy and Security and the Ministry of Foreign Affairs, which is being implemented in 2023-2024.

multidisciplinary approach to creating public policies. Global security challenges: regional and local conflicts, ethnic and religious extremism, terrorism, organised crime, proliferation of weapons of mass destruction, illegal migration, hybrid threats, cyber threats, limited availability of natural resources, including water, food, energy and raw materials, as well as climate change and environmental degradation, threaten the stability of individual states and entire regions, as well as global security (SNB, 2019).

In such security conditions, the Republic of Serbia, like some other small European states, bases its foreign policy orientation on the development of political and economic ties with partners of different ideological approaches and opposing geopolitical positions and on reliance on military neutrality, which primarily refers to non-adherence to military alliances and a neutral attitude towards parties to armed conflicts. Despite some perceptions that neutrality has lost its realistic function in preserving sovereignty and autonomy, it continues to serve as a bearer of national identity for neutral states and as a promoter in international peacebuilding (Goetschel, 2011).

Neutrality is defined as strategic independence in relation to powerful states, and such a foreign policy status requires compliance with certain rules of conduct in international relations (Vračar and Čurčić, 2022: 46). Political neutrality is in today's conditions more in the domain of a theoretical concept than reality, as it implies non-alignment and non-belonging to political (and economic) organizations in which certain interests of the state would be realized, the creation of other formal political alliances that in some domain exclude the independent conduct of the country's policy, or alignment with a side in a conflict without formal alliance (Trapara, 2016; Gordić & Petrović, 2019). Military neutrality is a political decision that implies a state's conscious renunciation of military alliances, participation in wars and assistance to warring parties, as well as the obligation to defend military neutrality if it is threatened, including by armed means (Blagojević, 2022: 233). The creation of military neutrality as the most important component of political identity aims to ensure the security of the state from the influence of external factors. Regardless of the controversial understandings of neutrality and frequent discussions about the principles of military neutrality, especially the actions of certain neutral states during World War II, it cannot be denied that a military neutral status does not have an offensive, but rather a peacetime character.

GLOBAL SECURITY RISKS AND THREATS

Current international relations are largely dominated by tensions between great powers and the formation of blocs, rather than the spirit of multilateral cooperation. The absence of a supreme authority at the international level means that states are forced to act in a way that best ensures their security, otherwise they will be in a position where they risk being threatened (Walt, 1987). The spread of globalization and economic inter-

dependence has shown that ethnic, ideological and religious identities have not weakened, but have created such social differences that have fueled a wave of civil wars and secessionist aspirations (SFRY, Chechnya, Georgia, Ukraine, Moldova), the spread and deepening of terrorism (Iraq, Syria, Afghanistan, Moscow, Paris), but also the emergence of new challenges and security threats (cyber-attacks in Iran) (Mišev, 2020: 151). This state of affairs on the international stage led to the first war on European soil in the 21st century. The armed conflicts in Ukraine, starting in 2014 and the non-compliance with the Minsk Agreements (2014 and 2015), destroyed the security architecture in Europe, which was based on trust and cooperation. The idea of a single European area of cooperation and security that includes Russia was unsuccessful, and the European concept of state security is being questioned. The introduction of several packages of sanctions against Russia, the increased influence of the United States on Western European countries and their material, financial and military support for Ukraine, interruptions in the supply of energy and other necessary material resources from Russia, as well as very unfavorable political relations, have had a negative impact on the economies of Western European countries, and have not contributed to the cessation of hostilities in Ukraine.

The influence of global power centers is a constant and dynamic process that indirectly affects the rest of the world. Russia seeks to regain its political, economic and military influence in Europe, the Middle East and Africa, especially in countries with neo-colonial influence of Western European states, but also to preserve its security by limiting NATO's further advance to the east (Ukraine, Georgia, Moldova). On the other hand, the US and its strategic partners in Europe want to maintain the *status quo* in international relations and expand their influence over European states that pursue independent or pro-Russian policies. China is trying to use its economic influence and the conflict between the US and Russia to take a leading position in the global system, both in the Indo-Pacific and in Europe, America and Africa. Considering that China is the only great power that has not waged a single war for more than 40 years (after the one-month war with Vietnam in 1979), implementing the Confucian model of cooperation as a set of ethical principles, it is becoming an increasingly important factor in international relations and an increasingly desirable economic, military and political partner. In this way, the share of non-military means for achieving political and strategic goals has not only grown, but has sometimes proven to be more effective than traditional military weapons (Mišev, 2020). The growth of economic and military capabilities of states that claim to be great powers causes intense competition among them in the sphere of resource exploitation and market dominance, as well as in the exercise of military and political power (Schweller & Pu, 2011). Regional powers such as Turkey, India, and Brazil are also seeking to expand their scope of action with the aim of changing the global order.

The overall security situation in the world has become more unstable, complex and unpredictable in the last decade, with a large number of armed conflicts⁵, with international governmental institutions, including the UN Security Council and the UN as a whole, demonstrating disunity and ineffectiveness in acting to de-escalate conflicts caused by the state policies of the great powers. Based on a comprehensive analysis of the security environment, the question arises to what extent European states, including Serbia, need to adapt their security policy and its instruments in order to be able to respond quickly and adequately to changing security threats and dangers in order to protect national interests. Kenneth Waltz believes that security is one of the key national interests of every state. National interest implies a set of values that are protected, primarily sovereignty, independence, territorial integrity, national identity, constitutional order, freedom, etc. (Waltz, 1987). Continuous monitoring and analysis of the strategic environment at the global, regional and national levels identify challenges, risks and security threats that are assessed to have, or in certain circumstances may have, a direct or indirect impact on the security of citizens and the state. At the same time, priorities are determined in the function of protecting national interests, and in order to take preventive and appropriate measures to develop the capabilities of the defense and security system. As a result, public policies of strategic interest for security are created and implemented not only at the national, but also at the regional and global levels.

POLITICAL IDENTITY AND STATE NEUTRALITY

The crisis of building an independent political identity has never shown such dependence on great powers, not even during the Cold War, when the politics of the Non-Aligned Movement played a serious role in international relations. Identity politics suggests a political orientation built around an existing social identity (Ford, 2005). Territory, language, ideas, culture and history can serve as objects upon which to establish notions of political identity. Political identity is used as a tool to make political claims, promote political ideologies or stimulate and orient social and political actions, usually in a broader context of inequality or injustice and with the aim of affirming group distinctiveness and belonging and gaining power and recognition (Neofotistos, 2013). In short, political identity can be defined as a form of social identity that marks membership in certain groups that share common interests with the aim of retaining and increasing power.

The formation of a European political identity shows that Europe is integrated into a wider global community through the World Trade Organization (WTO), the UN, NATO,

⁵ Armed conflicts affected 56 countries in 2022. Major conflicts, with over 10,000 deaths, were in Ukraine, Myanmar and Nigeria (probably also in Ethiopia, but there is no confirmation of the number of victims), intense conflicts in 16 countries (with 1,000 to 9,999 deaths), while in other conflicts the number of victims was lower. The total number of estimated conflict-related deaths was 147,609, which is slightly less than in 2021 (Stockholm International Peace Research Institute, 2023).

etc. In considering the notion of a European identity, rather than the subsumed national identities of European constituent states, peripheral territories can present aggravating circumstances, as in the case of the Partnership for Peace countries. Despite the attempts of the European Union to create a distinct identity for Europeans, there are other centripetal and centrifugal forces working to create broader and narrower political identities, because the European identity is not like the Partnership for Peace program within the framework of a new world security order (Bryder, 2005: 45). The attempt to create a Euro-Atlantic or Western political identity based on military power implies imposing an equal political identity on all European states. History has shown that political science and security studies on the development and building of nation-states have had a constant tendency to form political collective identities: economic (EC, EU, WTO, OECD), political and legal (UN), as well as military (Warsaw Pact, North Atlantic Treaty Organization, Axis Powers, Entente Powers).

During the formation of the nation-state, almost all European governments took action to "homogenize" their populations in terms of religion, ethnic and cultural minorities, national language, and public mass education system (Nevola, 2011). Governments that did not take such action failed to achieve it, creating very fragile and insecure nation-states, as happened in Southeast Europe. This created problems with identity politics, and this failure created major problems with national identity, and therefore for the nation-state. Political identity and national identity are essential components of the political culture of a society (Nevola, 2011: 39).

The modern European order, under the guise of a European economic and political identity, is imposed through the European Union and NATO. Most European countries have accepted to identify themselves through these two organizations, so that the EU currently has 27 members and NATO 32. Even militarily neutral states (Austria, Switzerland, Sweden, Ireland, Serbia, Bosnia and Herzegovina, Moldova, Ukraine, Russia) have joined NATO's Partnership for Peace program. This tendency is best explained by the theory of political unification. The theory of political unification emphasizes that collective identity needs "force" if it is to be a resource for the "political unification" of a community; in other words, it must be supported by power structures and instruments that bind affiliation and translate identity into loyalty. In this case, the availability of political identity is confirmed and collective loyalty is established, which consists of the possibility of setting a "common bond" as binding (political obligation) (Nevola, 2011). In this way, great powers use international organizations to project power with the aim of exercising direct control and influence on the creation of public policies of member states. Equating national identity policies with the policies of powerful actors in the international system makes it impossible for states to conduct sovereign and independent foreign and domestic policies and build their own national political identity.

Figure 1. *Eurasian Corridor*



Source: *Google Maps*.

Since global power centers do not enter into direct conflicts, the struggle for spheres of influence takes place in countries that are not sufficiently resilient to global changes and upheavals. In a move from Israel and Palestine, through Syria, Azerbaijan, Georgia to Ukraine, the Eurasian War Corridor was created in place of the former Iron Curtain. The struggle over the division of spheres of influence and the imposition of their own political, but also economic and cultural identity by global power centers proved to be a source of instability for independent states. The end of the Cold War led to armed conflicts in which the great powers measured their strength. The fragmentation of the European federal states of the USSR, the SFRY, Czechoslovakia, but also the unitary republics of Moldova, Georgia, Ukraine, Azerbaijan, and Syria, has shown that there is no region that is not sensitive to changing geopolitical relations and changing constellations of power in the process of multipolarization. The war in Ukraine has caused Western European states to fear Russia and a possible new conflict, which has also caused a wave of reconsideration of the foreign policy orientations of states, especially among the Nordic countries.

NEUTRALITY OF EUROPEAN STATES

The policy of military neutrality is an increasingly frequent topic of expert and scientific discussions. The abandonment or significant redefinition of the underlying postulates of neutrality has prompted serious challenges to the importance of neutrality, the authenticity and scope of the strategic culture of neutral states. For some, this concept is

outdated, while others believe that it can still contribute to strengthening peace and stability in the world. However, although radically modified, neutrality has not disappeared but continues to represent a concept that is an important segment of international politics (Stojanović, 2020: 211). A militarily neutral state may not be a member of a military alliance or participate in an armed conflict as a belligerent, except in self-defense, and is obliged to promote and encourage peace processes. This has contributed to militarily neutral states participating in UN peacekeeping missions, but also to building joint military capacities through the Partnership for Peace program or the Nordic Alliance.

After decades of development of the Nordic peace policy and military neutrality of Sweden and Finland, the return of Russia as a major military and political power shook the foundations of the security policy through which these states had built a clear political identity. Sweden bases its policy of neutrality on tradition, not on an international treaty. Neutrality was formally declared by King Gustav XIV in 1834. During the military conflicts of the first half of the 19th century, Sweden maintained its neutral status. Since World War II, Sweden's security has strongly depended on the status of Finland and indirectly on the policy of the USSR towards Finland (Finlandization). Like Finland, it became a member of the EU in 1995. Finland derives its policy of neutrality from the period immediately after World War II. Its interest in remaining neutral in conflicts between the great powers was first recognized in the Treaty of Friendship, Cooperation and Mutual Assistance between Finland and the USSR of 1948 (AFCMA, 1948). The treaty prohibited signatories from joining a military alliance against another signatory, and Finland was not allowed to allow its territory to be used to attack the USSR. Finland was also obliged to maintain its neutrality by means of adequate armed forces, which it used to cooperate with its neighbours. Military cooperation between the Nordic countries began after World War II, when Denmark, Norway, Sweden and Iceland formed the Nordic Council in 1952. Since the 1960s, Finland has joined and military cooperation has been intensified through several regional agreements: the Nordic Group for Cooperation on Military Matters of the UN (1960), which was changed to the Nordic Coordinated Arrangement for Military Peace Support (1997) (NORDEFECO, 2024). The Nordic countries have built their political identity through the development of the so-called Nordic peace policy, despite the fact that Iceland and Norway are members of the military-political international organization - the North Atlantic Treaty Organization (NATO). The specificity of the Nordic peace is that it was strengthened during the Cold War, when the Nordic region managed to remain excluded from high-tension activities and did not support the deployment of foreign troops and nuclear weapons despite their strategic orientation and the nearby military presence of both the Soviet and American superpowers (Mišev, 2022). Since the 1990s, the Nordic countries have been promoting military partnership through the Nordic Armaments Cooperation - NORDAC (1990) and the Nordic Defence Support - NORDSUP (2008) (NORDEFECO, 2024). All Nordic countries have a law on compulsory military service for men, and in Sweden and Norway also for women.

For security and political analysis, it is very significant that after the collapse of the USSR, Finland intensified its cooperation with the West, first in 1994 when it joined the NATO Partnership for Peace program, and then in 1995 when it became a member of the EU. This was not an obstacle for the Nordic countries to deepen their military and economic cooperation. In 2009, the Nordic countries signed a Memorandum of Understanding between the five Nordic nations, which established the Nordic Defense Cooperation - NORDEFECO. The specificity of this Memorandum is that it opened the way for cooperation with countries outside the Nordic region (NORDEFECO, 2024). Although the Nordic Defence Alliance did not expand, the Memorandum foresees respect for the UN, NATO and the EU, as well as cooperation with non-members of NORDEFECO, in particular Lithuania, Latvia and Estonia (NORDEFECO, 2024). Global changes, the disappearance of the Warsaw Pact, the strengthening and expansion of the NATO Pact and the increase in the number of secessionist wars, have contributed to the Nordic countries, primarily Sweden and Finland, changing their security policies. Due to increased tensions in Europe, as a result of the war in Ukraine, Finland and then Sweden became members of NATO after submitting applications.

There are no strategic military targets in Finland that would be a reason for an armed attack by another state. The geostrategic and security importance of Finland lies in its geostrategic position, as it shares a border with Russia for about 1,300 kilometers. Due to the increasing approach and expansion of NATO to the Russian borders, first Azerbaijan, Moldova and Georgia, and then Syria and Ukraine have been drawn into proxy wars with the aim of hindering the influence of the United States. In the modern constellation of power, where proxy wars are also being waged on European soil, Finland has objective reasons to be concerned about its security. Sweden does not border Russia, but in the changed geopolitical relationship, security threats, by their military and non-military nature, are not only territorial, but also supranational, multidimensional and multiplied.

Unlike Sweden and Finland, most of the militarily neutral states of Europe (Austria, Switzerland, Serbia, Bosnia and Herzegovina, Moldova, Cyprus, Ireland, Monaco) have retained their foreign policy direction and established political identity. All of these states are surrounded by NATO members and territorially far from global centers of power. In the case of Sweden and Finland, the policy of military neutrality is shaped as a foreign policy doctrine, while Austria and Switzerland are bound to neutrality by international treaties. Austria became neutral after its defeat in World War II on 26 October 1955 by the Vienna State Treaty (Treaty, 1955). Austrian military neutrality is based on three principles: military non-interference in the conflicts of other countries, a ban on the stationing of foreign troops in Austria, and non-adherence to a military alliance (Austrian security, 2023). As an EU member state, Austria has committed itself to gradually improving its military capabilities and to making civilian and military capacities available to the European Union for the implementation of common security and defence. Its security policy

is based on the EU document: *the EU Strategic Compass for Security and Defence*, which it has integrated into the Security Strategy 2023 (Austrian Security, 2023). Austria relies on security policy within the framework of the UN, the EU, the OSCE, its partnerships with NATO and within the Council of Europe. Austria is concerned that emerging global powers (Russia, China) pose a serious security challenge. It also believes that the lack of stability and prosperity in the peripheral areas of Europe negatively affects its security.

Switzerland's neutrality was recognized at the Congress of Vienna in 1815. Switzerland bases its neutrality on the strategy of "Security through Cooperation"⁶. The basic principles of Swiss neutrality include the prohibition of supporting parties to an international armed conflict, with the aim of avoiding armed conflict and maintaining impartiality⁷ (Security policy, 2021). Neutrality does not prevent Switzerland from cooperating militarily with other states and organizations where this is beneficial to both parties. In Europe, this primarily concerns the Partnership for Peace and the EU, and at the global level, it concerns cooperation with the US, Russia and China. There are warnings that the risk of direct military conflict between NATO and Russia has increased, leading to serious risks of escalation and ultimately potentially catastrophic consequences for Switzerland's security environment. South-eastern Europe continues to face tensions. In the Western Balkans, the EU's rapprochement has a stabilizing effect on the region, although the potential for conflict remains on the ground, for example in the relations between Serbia and the so-called Kosovo, as well as within Bosnia and Herzegovina (FDD, 2021). Like Austria, Switzerland emphasizes the high risk of conflict between global centers of power and Southeast Europe as a potential flashpoint in this relationship.

International relations in the new geopolitical and geostrategic paradigm, characterized by the opposing dynamics of globalization and fragmentation, show that the creation of political identity is a continuous and never-ending process. Europe faces numerous security challenges. In addition to the war in Ukraine, the threat of nuclear and hypersonic weapons, cyberattacks, the spread of terrorism, illegal migration, climate change, pandemics, Europe is struggling with increasing internal problems such as unstable financial markets and the strengthening of right-wing movements. In the last ten years alone, Europe has faced referendums on independence in Scotland (2014) and Catalonia (2017), and the peak of political turmoil was the UK's departure from the EU

⁶ This principle ensures that if Switzerland is the target of an armed attack, it has both options available: autonomous defense or cooperation with other states, especially its neighbors.

⁷ The sustainability of Swiss neutrality has been questioned several times in the past. Thanks to economic concessions with Germany and the general development of events during World War II, it managed to maintain its neutral status. Due to the military operations in Ukraine, Switzerland joined the sanctions imposed on Russia by the EU countries, which its leadership does not interpret as a departure from the policy of neutrality, but as compatibility of its own policy with the EU, since it does not provide military assistance to any of the warring parties, despite pressure from Western countries to allow the export of military equipment to Ukraine (Đukić and Vuletić, 2023: 626).

(Brexit). It is obvious that the politics of national political identity are strengthening. On the other hand, out of fear of conflict between opposing centers of power on a global scale, after the historic expansion of seven countries in 2004, NATO has been strengthened in the last decade with four more countries, including Finland and Sweden. With complex global security challenges and changing geopolitical relations, states cannot rely solely on their own armed forces.

CHALLENGES TO THE MILITARY NEUTRALITY OF THE REPUBLIC OF SERBIA

Serbia's military neutrality stems from a strategic commitment based on the National Security Strategy and the Defense Strategy, both from 2019. The strategies indicate how the state will use national power in accordance with state policy (Lykke, 2001). In order for the holders of political power to determine the instruments and mechanisms for defending national interests, it is necessary to define threats to the security of the state.

Challenges, risks and threats to security, of a military and non-military nature, which in certain circumstances may endanger the peace and stability of Serbia and the region, are defined by the National Security Strategy: (1) armed aggression; (2) separatist tendencies; (3) the illegal unilateral declaration of independence of "Kosovo"; (4) armed rebellion; (5) terrorism; (6) proliferation of weapons of mass destruction; (7) ethnic and religious extremism; (8) intelligence and subversive activities; (9) organized crime; (10) drug addiction; (11) illegal migration; (12) problems of economic development, (13) problems of demographic development; (14) epidemics and pandemics of infectious diseases; (15) endangerment of energy security; (16) the unfinished process of demarcation between the states of the former SFRY; (17) the consequences of natural disasters and technical and technological accidents, as well as the threat to the environment and the health of citizens due to radiological, chemical and biological contamination and (18) climate change and (19) high-tech crime (SNB, 2019). The general state of security in the world is also significantly threatened by gross violations of the UN Charter and generally accepted norms of international law, in particular interference in the internal affairs of sovereign states, as well as the concept and practice of pre-emptive attack and military interventionism. Of particular concern is the tendency to aggravate relations between great powers, conditioned by competition for the realization of their opposing interests and the change of existing spheres of influence. In such circumstances, the risk of a military conflict on a global scale, although significantly reduced, cannot be completely ruled out (SNB, 2019). The dangers of an armed attack on Serbia and the outbreak of armed conflicts in the region depend on the relations between the great powers and the possibility of their direct confrontation.

For Serbia, the most significant security issue is the still unresolved status of the Autonomous Province of Kosovo and Metohija (K&M) and the constant tensions caused

by the provisional Pristina institutions. The protection of sovereignty, independence and territorial integrity is possible only if the Government has control over its entire territory, which is why K&M remains the primacy of Serbia's security policy. K&M in this sense represents a dual type of security challenge for Serbia, which adds another type of complexity to this issue. First, the potential for renewed conflict in this area represents a direct challenge to Serbian security and Serbian policy of neutrality. On the other hand, military neutrality can become challenging in situations of tension or conflict, as global power centers use the situation to project their power and expand their influence. Given that the provisional institutions of government in the southern Serbian province are supported by the US and NATO, and that all countries surrounding Serbia are NATO members (except Bosnia and Herzegovina), there is pressure from NATO countries that have taken clear positions in support of the independence of Kosovo and Metohija, which may lead to tensions in maintaining Serbia's neutrality. In addition, changes in regional relations such as the influence of China and Turkey and sudden events, such as the war in Ukraine and the Middle East, may pose challenges in maintaining political identity, especially if the situation changes rapidly.

It is clear that Serbia's biggest security problem is not Kosovo and Metohija, but the conflicting interests of the great powers in Southeastern Europe, especially Serbia, which is a challenge for the whole of Europe. Also, unresolved relations with the countries of the former SFRY and energy dependence on Russia further undermine Serbia's commitment to European integration. With its geographical location, road, river and rail transport network, Serbia has the potential to become the logistics center of the region (Stanojević, Mišković and Mišev, 2017). In economic and political terms, Serbia must rely on cooperation with the EU's largest foreign trade partner, but also with the USA, Russia, China and Turkey. Therefore, its foreign policy activities are focused not only on EU membership, but also on the development of bilateral and multilateral economic and political relations. Serbia's advantage in the process of resolving the status of Kosovo and Metohija is its membership in international organizations, primarily the UN, and the preservation of the principles set forth in the UN Charter and UN Security Council Resolution No. 1244 as an important foreign policy action of Serbia. Participation in and respect for military and economic-political alliances such as NATO, the SCO and the CSTO definitely show that Serbia has a friendly and defensive policy towards other states and alliances. However, countries aspiring to become NATO members are expected to meet certain political, economic and military conditions in order to ensure that they become security partners of the Alliance, and not just its beneficiaries. Among other things, like EU membership, NATO membership is conditioned primarily by territorial integrity and control of the entire territory and borders. Therefore, joining NATO in its current strength would require Serbia to give up part of its territory in order to meet the conditions for full membership. This means jeopardizing a vital national interest defined by public policies, which are, among other things, deeply rooted in the historical and national consciousness of Serbian citizens.

The unresolved status of Kosovo and Metohija is only a reflection of the lack of a consistent international policy and international law on European soil. The same applies at the global level, taking into account the situation in Israel and Palestine, Syria, Afghanistan, Somalia, Sudan, Libya. The priority of European states should be a common identity policy constituted and created through the EU. However, international institutions have become an instrument of power in the hands of global centers of power with the aim of realizing their interests. From all of the above, it is clear that new security threats are creating conditions for the formation of a new international order, primarily due to distrust and competition among the great powers, which is an obstacle to building a common policy of global peace. The current structure of the international order is not and must not be an obstacle to the national defense strategy of Serbia, which is based on military neutrality. If Serbia were to opt for a military alliance, in this case NATO, it would clearly jeopardize vital national interests, which is the preservation of Kosovo and Metohija. Therefore, it is undeniable that military neutrality is an adequate political framework for defending Serbia's national interests and preserving peace in this part of Europe.

CONCLUSION

In essence, the most dangerous threat to Serbia's military neutrality is the complex interplay of geopolitical pressures, unresolved regional conflicts, and the evolving nature of security threats. Navigating these challenges requires a delicate diplomatic approach, strategic foresight, and a commitment to preserving Serbia's sovereignty in the face of complex regional dynamics. Effectively managing these challenges requires careful diplomatic and military strategy to preserve military neutrality while maintaining stability and security in the region.

Europe has shown itself unable to resist the political pressures of global power centers, which is why peripheral states in particular are at risk of destabilization. The European political identity has been incorporated into NATO, which has not only deprived states of the ability to conduct an independent foreign and defense policy, but the EU itself has not built its own military capabilities independently of the military alliance. With its rapid expansion, NATO has made a strategic shift towards Russia, which resulted from the US strategy of maintaining global primacy, limiting the strengthening of the military forces of European states or the joint armed forces of the EU, increasing military potential and securing other resources from new members. Serbia is located in a region with historical conflicts and tensions, with pressures from various international actors who want to draw it into certain alliances or provoke new conflicts. Maintaining effective defense within the framework of military neutrality is becoming increasingly demanding. Military neutrality can cause difficulties in building relations with other countries, especially those that are members of military alliances. Serbia must balance

between preserving military neutrality and cooperating with various states and international organizations in order to protect national interests, primarily preserving sovereignty and territorial integrity. Maintaining military neutrality in the context of preserving sovereignty is a challenge, especially in light of regional events and international tensions. On the other hand, Europe must redefine its political and economic role, both at the regional and global levels, and resist dependence on global centers of power.

REFERENCE LIST

AFCMA. (1948). *The Agreement of Friendship, Coöperation, and Mutual Assistance between The Union of Soviet Socialist Republics and The Republic of Finland*. Retrieved December 6, 2023, from http://heninen.net/sopimus/1948_e.htm

Aunesluoma, J. & Rainio-Niemi, J. (2016). Neutrality as Identity: Finland's Quest for Security in the Cold War, *Journal of Cold War Studies*, 18(4), 51-78.

Austrian Security. (2023). *Austrian security strategy*. Retrieved December 12, 2023, from <https://www.bundeskanzleramt.gv.at/themen/sicherheitspolitik/sicherheitsstrategie.html>

Blagojević, V. (2022). Iskustva i izazovi Srbije u realizaciji strateškog odvrtaćanja. U V. Blagojević (ur.), *Neutralnost i strateško odvrtaćanje* (pp. 229-245). Beograd: Medija centar „Obrana“.

Bryder, T. (2005). European Political Identity An attempt at conceptual clarification. *Psicología Política*, (31), 37-50.

Đukić, A. i Vuletić, D. (2023). Organizacija sistema odbrane prema konceptu totalne odbrane na primeru Švajcarske, Švedske i Srbije. *Međunarodni problemi*, 75(4), 621-647.

FDD. (2021). *The security policy of Switzerland*. Retrieved December 02, 2023, from Federal Department of Defense: [html/vbs-internet/en/documents/security-policy/security-reports/2021/sipol-b-2021-e.pdf](http://www.fdd.ch/en/documents/security-policy/security-reports/2021/sipol-b-2021-e.pdf).

Ford, R. T. (2005). Political Identity as Identity Politics. *Unbound*, 53(1), 53-57.

Goetschel, L. (2011). Neutrals as brokers of peacebuilding ideas? *Cooperation and conflict*, 46(3), 312-333.

Gordić, L. M., & Petrović, B. I. (2019). Model of military neutrality as perspective of development of the Republic of Serbia“. *Baština*, 47, 117-134.

Lykke, A. F. (2001). Toward an Understanding of Military Strategy. In J. Joseph R. Cerami & James F. Holcomb, *U.S. Army War College Guide to Strategy*. U.S. Army War College. 179-185.

Mišev, G. (2020). Teorijski dometi izučavanja energetske bezbednost kao globalnog izazova u međunarodnim odnosima. *Sociološki pregled* vol. LIV, no.1, UDK 327:620.9 (100). Beograd. 149-173.

Mišev, G. (2022). *Faktori uspešnog razvoja država i njihove implikacije na bezbednost*. Doktorska disertacija, Univerzitet u Beogradu, Fakultet bezbednosti.

- Neofotistos, V. (2013). *Identity Politics*. London: Oxford University Press.
- Nevola, G. (2011). Politics, Identity, Territory. The “Strength” and “Value” of Nation-State, the Weakness of Regional Challenge. Italy, Trento: University of Trento, *Department of Sociology and Social Research*. Volume 58.
- NORDEFECO. (2024, 1). *Nordic Defence Cooperation*. Retrieved December 10, 2023, from NORDEFECO: <https://www.nordefco.org/the-basics-about-nordefco>
- Schweller, R., & Pu, X. (2011). After Unipolarity - China’s Visions Of International Order. *International Security*, 36(1), 41–72.
- SNB. (2019). *Strategija nacionalne bezbednosti Republike Srbije*. Službeni. glasnik RS, br. 94/2019).
- Stanojević P., Mišković V. & Mišev G. (2017) *Nacionalna logistika i bezbednost*, Fakultet bezbednosti, Univerzitet Beograd.
- Stockholm International Peace Research Institute. (2023). *Trends in armed conflicts*. Retrieved January 10, 2023, from: <https://www.sipri.org/yearbook/2023/02>
- Stojanović, C. (2020). Savremena strateška kultura i neutralnost. *Vojno delo*, 72(4), 210-233.
- Trapara, V. (2016). Finlandizacija kao model neutralnosti malih država. *Međunarodni problemi*, 68(4): 351-389.
- Treaty, S. (1955). *The 1955 State Treaty and Austrian Neutrality*. Retrieved December 25, 2023 from <https://countrystudies.us/austria/47.htm>
- Vračar, S. M. i Ćurčić, T. M. (2022). Vojna neutralnost Republike Srbije kao strateška kategorija. *Srpska politička misao* (posebno izdanje), 41-65.
- Walt, S. M. (1987). *The Origins Of Alliances*. New York: Cornell University Press.

Milan Miljković¹

Hatidža Beriša²

Dejan Petrović³

CHARACTERISTICS OF MODERN CONFLICTS IN THE INFORMATION SPACE AND THEIR APPLICATION IN THE DETERRENCE STRATEGY⁴

Abstract

In modern conflicts, the use of information warfare is actualized, as a way of conducting geopolitical conflicts between great powers, but also as a means of strategy of coercion and deterrence. On the other hand, modern information technology provides the opportunity for other participants in the conflict, primarily non-state actors and small states, to influence the informational dimension of the conflict, and thus the decisions of the great powers regarding the use of military force. The aim of the paper is to review the relevance of the classic theoretical approach to the use of information warfare and its application in the deterrence strategy. In the paper, the subject of research is considered through the application of the method of comparative analysis of theoretical and doctrinal positions of military thought in the Russian Federation on information warfare and deterrence strategy, with the results of their application in modern conflicts, such as the conflict in Ukraine on February 24, 2022. The authors assess that, bearing in mind that the adversary leaders are the central target towards which the strategy of coercion and deterrence is directed, deterrence must be understood primarily as an effort to shape the thinking of the leader of a potential aggressor, the perception and behavior of the opposing armed forces, the population and the international community. In this regard, the results of the research, especially the application of information deterrence measures in the conflict in Ukraine during 2022 and 2023, point to the conclusion about the relevance of the application of information warfare for today's practice of the deterrence strategy.

Keywords: *information warfare, strategy, deterrence.*

¹ School of National Defense, University of Defense in Belgrade, Serbia, milanmiljkovic04011@gmail.com.

² School of National Defense, University of Defense in Belgrade, Serbia

³ School of National Defense, University of Defense in Belgrade, Serbia

⁴ The paper was prepared as part of a scientific project of the National Defense School "Vojvoda Radomir Putnik" of the University of Defense entitled "Neutrality and Strategic Deterrence", ŠNO-DH /22-24.

CONFLICTS IN THE INFORMATION SPACE - INFORMATION WARFARE

Information has always been a means of exerting influence, and modern information technology allows people to produce and share more information and organize themselves faster than ever before in history. One of the main challenges we face in modern society, but also a key driver of activity in it, is the dramatic and constant diffusion of information and technology used by both states and their security forces involved in conflicts, as well as smaller and non-state actors. The rapid spread of information calls into question the ability of some states to control their populations and maintain internal political stability (Ehlers, 2017). The diffusion of power through the use of information and information technology has enabled individuals and groups to participate in and influence the global information sphere. The ability to act on information for the purpose of social and political change was once the exclusive ability of nation states. However, today, individuals also have the ability to create, transform and disseminate information on a global scale in order to mobilize social and political activities and changes. In this regard, it should be emphasized that information warfare is one of the basic forms of influence and conflict in the information society.

In modern conflicts, the use of information warfare has become relevant not only for conducting non-military and military operations, but also in strategic concepts of deterring the enemy. Information warfare is used to act on enemy information and information systems, and sources of information, but also to change the mindset of the opposing side (Miljković & Jevtić, 2021). The primary goal of information warfare is the enemy leadership, specifically the decision-making process of the opposing leadership. By reducing the opponent's ability to make timely and effective decisions, the opponent's response or initiative towards the activity carried out by the opposing side is reduced.

The development of the information environment also develops ways of influencing the enemy and waging information warfare (Nezhdanov, 2021). Information warfare is implemented by conducting information operations. Definitions of information operations are primarily present in the security and military doctrinal documents of Western countries and China, while theorists of the Russian Federation use the term *информационная война* (information war) or information warfare (Panarin, 2012). The term *information operations* is accepted in doctrinal documents of the USA and EU countries, and as such already exists in the current Doctrine of the Serbian Armed Forces (Doktrina Vojske Srbije, 2010).

According to the above, information operations can be defined as activities that influence the information, systems and sphere of the enemy, while at the same time protecting one's own information, systems and sphere. Information operations include activities ranging from measures to prevent the enemy from exploiting information, to appropriate measures to ensure the integrity, availability and interoperability of one's own information resources.

When considering the *division* of information operations according to the means of execution, the approach of Russian theorists is significant, who advocate the position

that information actions are divided according to the means used into operations that are carried out: a) by information-technical means (attacks on critical objects of national infrastructure, cyber attacks) and b) by information-perceptual means, propaganda, management of the enemy's perception, disinformation, psychological operations and deception (Timothy, 1996).

Theorists Chekinov and Bogdanov argue that the increasing importance of information operations has changed the previous understanding of traditional kinetic operations as the "final measure of defeat" only after full information superiority has been achieved (Chekinov & Bogdanov, 2017). They and other Russian theorists argue that "information superiority" is now necessary to enable a successful kinetic operation (Dulnev & Litvinenko, 2016). Russian analysts argue that the success of "not only the initial phase of a military operation, but also the outcome of the entire campaign depends on a skillful, clearly calculated and reasoned" information operation (Pechurov & Sidorin, 2017). They assess that a kinetic operation cannot succeed without a successful information operation to enable it.

Modern conflicts, according to the aforementioned Russian views, are based on the idea that the enemy's mind is the main field of military and non-military competition. The goal is to impose decisions and activities on the enemy's army and civilian population that are in line with the interests of the attacker, to the detriment of the enemy state. As a result, new generations of military conflicts are predominantly informational and psychological in nature, since this is how control over the enemy's information sphere is achieved, the enemy's psychological state is depressed, and morale is reduced. By applying these actions, the need for a significant engagement of military forces in conflicts is reduced (Chekinov & Bogdanov, 2013).

The above theoretical views on the importance of information conflicts in new wars have influenced the further development of the concept of strategic deterrence, where information actions play an important role as an element of non-military measures of strategic deterrence, acting through two domains, both cognitive-psychological and digital-technological.

INFORMATION MEASURES OF STRATEGIC DETERRENCE IN THE MILITARY THEORY AND DOCTRINE OF THE RUSSIAN FEDERATION

The conceptual approach to deterrence of the Russian Federation differs from the Western conceptualization of this term, and the interpretation of this concept in the Russian strategic lexicon is much broader than the meaning that Western experts have in mind. In short, deterrence from the Russian perspective means the use of threats, sometimes accompanied by limited use of force, with the aim of a) maintaining the *status quo* ("deterrence" in Western parlance), b) changing the *status quo* ("coercion" in

Western parlance), c) shaping the strategic environment in interaction with other strategic factors, and d) preventing escalation or bringing about de-escalation (Adamsky, 2020: 161-175). The term is used to describe activities both before and during a military conflict, and encompasses all phases of war.

The concept of strategic deterrence of the Russian Federation, in the sense used in Russian military theory, is a holistic concept that envisages the integration of non-military and military measures to shape the decision-making of an adversary. This concept integrates the state's non-military instruments of national power and identifies specific military capabilities that are "strategic" due to the expected effects when used for deterrence purposes. According to the Russian view, strategic deterrence is an adaptable concept, as it can be applied to the management of unforeseen situations, ranging from local wars with a single state, through regional conflicts against coalitions, to large-scale wars against global nuclear-armed powers such as the United States (Kofman et al., 2020).

In the Russian concept of deterrence, the list of military deterrence measures is more extensive, indicating that it is a concept that primarily relies on the strong end of the coercive spectrum. Military measures range from demonstrations of military presence and power, raising readiness to war levels, deploying forces, demonstrating readiness within forces and assets intended to deliver strikes (including nuclear weapons), and carrying out or threatening to carry out individual strikes.

Non-military means include political, informational (psychological and technical), diplomatic, economic, legal, spiritual/moral, and humanitarian measures (Chekinov & Bogdanov, 2011). Common examples include the implementation of economic sanctions, the introduction of economic blockades, the formation of coalitions and alliances, the severance of diplomatic relations, and the conduct of information warfare (Gerasimov, 2013). Theorist Kondakov notes that the use of non-military means varies depending on capabilities, the political situation at a given time, and the current position in the spectrum of conflicts (Kondakov, 2022). According to authors Chekinov and Bogdanov, non-military measures offer a number of advantages in peacetime conditions, including deterring armed conflicts, stabilizing the international system, strengthening relations between states, and eliminating potential threats from the adversary. In the midst of a political-military conflict, non-military measures act to strengthen military actions by acting as a force multiplier, serving to weaken and reduce the strength and capabilities of the adversary, and even completely eliminating the military threat (Chekinov & Bogdanov, 2011).

Before proceeding with the analysis of information deterrence measures, it should be said that from 2000 to the first years of the second decade of the 21st century, two general types of military-strategic thought can be distinguished in Russian military theory. The first is traditional and conservative, and the second is newly emerging and innovative, within which the theory of conducting conflicts in the information sphere stands out (Miljković & Jevtić, 2021: 105-131).

Proponents of traditional military thought do not deny the emergence of changes in the content of war, but they believe that the role of the "non-military factor" in achieving final success in war, including the concept of strategic deterrence, has been exaggerated.⁵ Analyzing the texts of Russian military theorists and practitioners, it can be concluded that one of the most important representatives of the traditional view is General Valery Gerasimov, who advocates the position that strategic deterrence is primarily based on the application of military measures, which are supported by the application of non-military measures. According to him, the main content of military strategy consists of issues of preparations for war and its conduct, primarily by the armed forces. The army, in his opinion, has a coordinating role for the application of military and non-military measures, especially during temporary periods of peace. In Gerasimov's opinion, confrontation in other spheres (non-military) represents a separate area of activity with its own methods and strategies. The job of the Russian army is to coordinate, not direct, these activities and functions (Gerasimov, 2013).

A different perspective is present among representatives of innovative military thought, such as Chekinov and Bogdanov, who believe that one of the essential future roles of kinetic operations is to support information campaigns, which achieve the ultimate goal of war. According to their assessments, within the framework of the Russian concept of the "new generation of warfare" (*новое поколение войны*) and the concept of strategic deterrence, information deterrence measures play a central role. They assess that information has long enabled deception, surprise and intimidation (deterrence) of the enemy, but this effect rarely went beyond the framework of tactics. Today, however, thanks to the sophistication of information influence tools, "indirect approach" and "information warfare" can solve strategic goals in conflicts and significantly reduce the enemy's determination to resist our intentions (Chekinov & Bogdanov, 2010). Accordingly, information warfare is perceived in Russian theoretical circles as one of the primary tools of non-nuclear deterrence. The idea of strategic influence through information measures, rather than with massive military force, has become the essence of the New Generation of Warfare and military operations of the Russian army. The term "information deterrence" (*информационное сдерживание*) is not mentioned in the military doctrine of the Russian Federation, but is widely used in expert discourse and refers to both digital and cognitive-psychological aspects of combat. According to Russian experts, this type of coercion can, under the influence of the changing nature of war, provide strategic stability and shape the strategic calculation of the enemy during hostilities (Manoilov, 2004).

In Russian discourse, the term originally emerged as a reaction to the American discourse on cyber deterrence. Information (cyber) warfare is seen as one of the most

⁵ One of the most prominent proponents of traditional views in the development of military thought was the long-time president of the Russian Academy of Military Sciences, retired Army General Garev Akhmetovich (Махмұт Ахметович Гареев).

cost-effective tools of non-nuclear coercion due to its ability to produce strategic effects without massive kinetic devastation (Sharikov, 2013). Its appeal lies in its ability to produce a range of significant strategic effects. As such, information deterrence is a crisis management tool aimed at the leadership and population of an adversary that can prevent military aggression without the direct use of military force (Manoilo, 2004). "Psychological intimidation" can credibly deter an aggressor for a longer period of time, and in some cases even deter him from aggression altogether (Manoilo, 2012). Thus, "informational deterrence" can deter aggression and completely prevent the violent phase of the conflict. Russian thinking about informational deterrence is truly cross-cutting, because, according to Russian views, it aims to prevent not only informational (cyber) aggression, but can also coerce the adversary's behavior in other areas of activity, including kinetic conventional operations. Informational pressure (*информационное давление*) on the adversary, its armed forces, state apparatus, citizens, and world public opinion aims to create favorable conditions for strategic coercion. As an illustration of this position, Russian experts cite the US informational campaign that it conducted to prepare the conditions for regime change throughout the Middle East during the Arab Spring (Chekinov & Bogdanov, 2013).

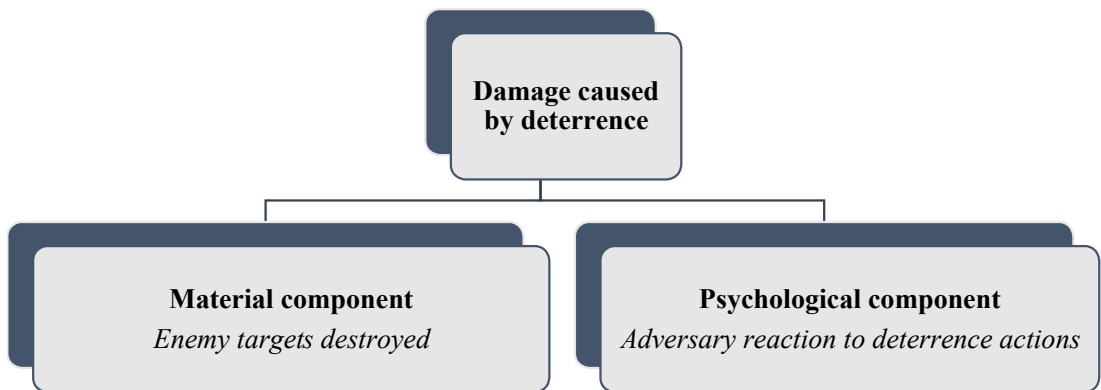
Russian experts believe that to achieve the effect of information deterrence, it is necessary to supplement the deterrence mechanism based on the digital-technological component of information warfare with a means of "reflexive control". In other words, "strategic information deterrence" includes digital-technological and cognitive-psychological forms of influence, through the threat of a massive special impact on the information resources of a potential adversary (Modestov, 2009). Unlike and beyond its nuclear or conventional analogues, information deterrence is a new form of strategic influence, based on a complex of interconnected political, diplomatic, information, economic, military and other means of deterrence, reduction and prevention of threats and aggression with the threat of unacceptable consequences. Preventive political-diplomatic activity, through effective information warfare aimed at preventing and resolving conflict situations, becomes the primary tool of strategic deterrence. Ideally, effective strategic coercion (both deterrence and coercion) should enable the achievement of political goals, without resorting to conventional military, let alone nuclear means, although their constant readiness and inclusion in the deterrence program is required (Gareev, 2009).

If non-military information deterrence actions are deemed ineffective, the state should switch to the use of "forceful deterrence" (*силовое сдерживание*) means with the aim of convincing the potential aggressor that the costs of aggression will exceed the expected benefits. To "insinuate" this to the potential aggressor, the Russian strategic community should: "demonstrate readiness" to deploy force groups in the expected zone of aggression, "ultimately announce the readiness of the Russian side to immediately use its nuclear weapons in the event of a threat to the sovereignty and territorial integrity

of the state," "announce the unlimited use of weapons of mass destruction to destroy" critical civilian nuclear-electronic, chemical, and hydropower infrastructure; and to replace and combine all of the above "to implement a special information operation to deceive the enemy about Russia's readiness to repel aggression" (Chekinov & Bogdanov, 2013: 23-24).

Furthermore, when considering the role of information operations within the Russian concept of strategic deterrence, it is important to consider the concept of “deterrent damage” in the current Russian military-analytical discourse. Thus, in Russian military journals, some analysts make a classification between "objective" (material) and "subjective" (psychological) concepts of deterrence damage (Roldugin et al, 2015). In this sense, "material" deals with real targets, and "psychological" with the impact on the adversary's will to continue with certain actions that the Russian leadership is trying to deter. This is shown in Scheme 1.

Scheme 1: *Classification of damage caused by deterrence*

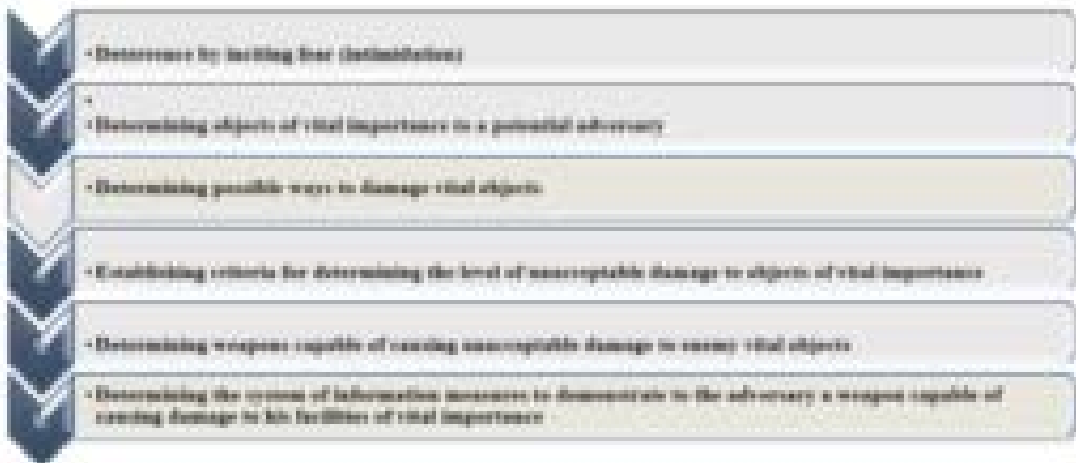


Source: D. Roldugin, Yu.V. Kolod'ko (2015), "A clarification of the concept of deterrent damage in resolving the tasks of deterrence through the use of force", *Strategic Stability*, No. 4/2015.

These analysts posited that the level of "deterrent damage" inflicted on an adversary could be progressively increased, "depending on the reaction to previous deterrent measures, as well as on the assessment of the degree of damage inflicted on each potential aggressor, given his views on national values, capabilities in defending national interests, and the sensitivity of society and the individual to possible losses" until finally “unacceptable damage” was reached. They contrasted "deterrent damage" and "unacceptable damage" in such a way that the structure and composition of deterrence potential should be oriented towards the guaranteed provision of a level of unacceptable damage. The concepts of subjective damage include the application of both informa-

tional action mechanisms and fear-mongering aimed at influencing the population and decision-making by the leadership (Burenok et al., 2009). For the purpose of informational action within the "subjective" (psychological) concept of deterrence damage, Russian theorists have also defined a methodology for developing a system of measures for informational deterrence, i.e. deterrence through fear-mongering (intimidation), which is presented in the table below.

Table 1. *Methodology for developing a system of deterrence measures through intimidation*



APPLICATION OF INFORMATION DETERRENCE IN THE CONFLICT IN UKRAINE

In the conflict in Ukraine during 2022 and 2023, the Russian Federation, in addition to military ones, also applied a certain number of non-military information measures of strategic deterrence, at the regional and global levels, so far with varying success.

Before launching a special military operation, the political and military leadership of the Russian Federation launched verbal and information threats with nuclear weapons, which Western theorists call "*signaling*" and which were then assessed as implicitly credible in Western circles (Ignatius, 2022). Thus, in December 2021, senior Russian officials warned that NATO's eastward expansion would trigger Russia's deployment of tactical nuclear weapons ("Russia Threatens to Deploy Tactical Nuclear Weapons", 2021). The rhetorical inclination towards escalation also appeared in the speeches of representatives of the Russian Federation on February 21 and 23, 2022, in which a special military operation was announced. Also, on February 27, 2022, President Putin stated that he was raising the readiness status of Russia's nuclear weapons due to Western threats ("Vladimir Putin Puts Russia's Nuclear Deterrence Forces On High Alert", 2022). Rhetorical threats

from the Russian political leadership continued in the following months, suggesting the possibility of nuclear escalation in the event of an "existential crisis" for Russia arising from the war in Ukraine ("A Kremlin Spokesman Says Russia Could Use Nuclear Weapons If There Is 'An Existential Threat For Our Country'", 2022). These threats inevitably regenerate Western fears of nuclear use and slow down allied responses to Russian special operations, allowing Russia to retain the initiative despite its military objectives on the ground not yet met. As a result of deterrence, Western efforts to provide full military assistance to Ukraine, such as sending NATO units to Ukraine, have been partially frozen. These threats are intended to intimidate NATO into intervening and to hinder efforts to strengthen NATO cohesion, to withhold significant arms supplies, and thus to isolate Ukraine so that Russia can retain the strategic initiative and dominance of escalation. Efforts at "intimidation" are constantly being implemented, including information warfare measures and actions against European states, with the aim of weakening the alliance between the United States and other NATO members.

When the Russian Federation launched a special military operation, Russian information operations expanded beyond the pre-February 24, 2022 narrative that justified military action, masked operational planning, and the start of the conflict. To win the information war and the military conflict, the Russian Federation launched an information campaign on multiple fronts against Ukraine with the aim of reducing its resistance and external support, including local, regional, and international public opinion.

It can be preliminarily concluded that the conflict in Ukraine shows that Russian information strategic deterrence is conceptually valid and has clear practical application, although it is obvious that the Russian Federation has failed to fully achieve the doctrinal prerequisites for a successful information campaign towards Europe and Ukraine, so that in 2022 there were mixed results in the effectiveness of the implementation of the Russian information campaign. A common observation is that the Russian Federation before and after February 24, 2022, failed to achieve the main goal of its theory and doctrine of information warfare, which is to achieve information superiority over the opposing side, both globally in relation to the USA and the EU, and regionally, i.e. in the territory of Ukraine, which negatively affected the effectiveness of the implementation of information deterrence measures. Conflict and deterrence in the information space in this conflict was conducted using information-psychological and information-technical means, i.e. operations in cyberspace, in the propaganda and intelligence field, as well as by competing in the field of mastering the enemy's communication systems. A preliminary conclusion is that the Russian side was expected to achieve much more results in terms of deceiving the enemy with cyber effects, propaganda activities in the field of strategic communication or influencing the enemy's communication on the battlefield, which is placed at the top of the list of goals in Russian military theory and deterrence doctrine.

If there was one area where the Russian Federation was expected to do the most, it was in its propaganda operations of influence conducted through both classical and modern media and cyberspace (Cordey & Sean. 2019). However, the violent dismantling and shutdown of Russian media outlets in the West and the EU, as well as the significant engagement of Western intelligence services in locating and removing social networks promoting pro-Russian views, contributed to Ukraine effectively parrying the information war for the support of the foreign and domestic Ukrainian public. In information operations, Ukraine managed to effectively turn everything from leaked, insecure Russian communications to videos of anti-tank ambushes into a narrative of triumph over the enemy. Ukraine waged a successful media war throughout 2022 that effectively portrayed the country as a victim and which at the time showed that Russia was paying a high price in the conflict.

As the conflict entered its second year, the Russian Federation's information operations continued their activities aimed at undermining international trust in Ukraine. With each narrative that is reinforced, whether through social media campaigns, the Russian Federation pursues its goal of undermining Ukraine until it gives up the fight. The results of this influence require time and positive results on the battlefield within the framework of a special military operation, which have already been partially achieved in mid-2023, with the capture of Bakhmut, as well as the subsequent conquest of Avdeyevka.

On the other hand, due to the aforementioned information blockade by the West, Russian propaganda has turned to the domestic Russian public and to opinion in the "third world" countries of Asia and Africa, in order to encourage the division of "the West against the rest of the world" and seems to have achieved some results in this area. In Europe and North America, where support for Ukraine generally remains high, it can be said that there are still contentious debates about supplying Ukraine with advanced weapons and additional funding. The Russian Federation, during this conflict, has been promoting "traditional family and Russian values" on a global scale, which has found acceptance in parts of Europe and the world among countries that are trying to preserve traditional values that are threatened by modern neoliberal views. China's global media ecosystem is also often biased towards Russian interests, while nations like India are working to maintain productive relations with both the Russian Federation and the West. In parts of Africa, anti-imperialist sentiment is manifesting itself in favor of Russia, where official Moscow presents itself as a friend and ally in the fight against historical colonizers such as France, which also leads to the overthrow of pro-Western regimes in some African countries. These examples are examples of the increase in Russia's international position and influence, and the positive results of its information campaigns on a global level towards the "rest of the world", while it continues to conduct a regional information campaign towards Ukraine.

CONCLUSION

The current Russian military theory and strategy of deterrence is an integrated complex of non-nuclear, information and nuclear types of influence contained in a single program for multiple domains. The above-mentioned approach to deterrence unequivocally indicates the increased importance of non-military and, within them, information deterrence measures, which together with military measures represent an integrated and holistic concept for shaping the decision-making of the adversary. The theoretical basis of this strategic and doctrinal approach was provided by the views of Russian theorists who indicate that the key to changes in future conflicts lies in the reversal of the historical pattern and role of non-military measures supporting military operations, that is, in modern wars, information campaigns support and influence the use of kinetic operations.

The continued development of the strategic concept of deterrence, which takes into account the more significant application of information measures, is also reflected in the views that today's strategic operations take advantage of the evolution of military technology used in offensive, defensive, information and other operations.

Actually, the current Russian theory and doctrine recognize four permanent strategic operations, which have integrated several others that existed before, but what should be especially emphasized is that some prominent representatives of Russian military thought emphasize the need to introduce a strategic operation in the sphere of information confrontation, i.e. strategic deterrence in the theater (sphere) of information warfare. The above indicates that the Russian articulation of the deterrence strategy continues to evolve. There is a strong desire to shape the cognitive space, placing emphasis on psychological, and not only material means of warfare. The Russian military therefore places emphasis on military cunning, technical means for shaping the enemy's decisions towards the desired actions and the functional defeat of the enemy's information systems.

It can be concluded that non-military and, within them, information assets occupy a prominent place in the Russian concept of strategic deterrence. They are crucial for actions or measures taken during the pre-conflict phase and for the strategy of deterrence and escalation management. Activities that fall within the domain of deterrence through information action are known in Russian military theory as information warfare and reflexive control. The conquest of information superiority must precede the immediate outbreak of war and is a condition for effective strategic deterrence. The struggle for information superiority begins in the peacetime period and ends generally by the end of the immediate preparation for launching the military phase of the war, i.e. at the end of the period of immediate crisis and war danger.

The analysis of the conflict in Ukraine also shows that Russia's non-nuclear strategic deterrence through the use of information measures is conceptually valid and has clear practical application, although the effects of the Russian Federation's information warfare in the conflict in Ukraine in 2022 and 2023 can be assessed as secondary

compared to the effects of kinetic weapons. The above-mentioned modest results of information action on opponents in Ukraine and Europe are a consequence of the fact that in practice the Russian Federation has not technically managed to do what theory and doctrine required, namely to achieve information superiority over the aggressor before the start of the conflict. The Russian Federation failed due to the fact that it did not technologically ensure that its information would be present in the Western information space, given the activities of Western countries to shut down and close Russian media outlets at the very beginning of the conflict, as well as due to the fact that Ukraine managed to remain on the Internet with the help of the West, which installed a new SpaceX's StarLink orbital information network over this country. In response to the aforementioned information sanctions, the Russian Federation turned to new and social media as channels for influencing Western and Ukrainian public opinion.

Also, everyday statements by high-ranking political and military representatives of the Russian Federation represent a practical application of theoretical positions indicating that deterrence must be understood primarily as an effort to shape the thinking of a potential aggressor. Deterrence policies are often viewed from the perspective of the deterring country, focusing on activities that are necessary to increase the costs and risks of an aggressor's attack. But the value of these actions depends entirely on their impact on the perception of the leader of the aggressor state, i.e. the party being deterred from aggression. Any strategy for deterring aggression must begin with an assessment of the interests, motives, and imperatives of the potential aggressor, including its theory of deterrence, and taking into account what the aggressor values and why.

REFERENCE LIST

Adamsky, D. (2020). Deterrence à la Ruse: Its Uniqueness, Sources and Implications, *Deterrence in the 21st Century - Insights from Theory and Practice*, NL ARMS Netherlands Annual Review of Military Studies.

Burenok V.M., Pechatnov Yu.A., Tagirov R.G. (2009). On the issue of determining the levels of unacceptability of consequences when solving the problem of forceful strategic deterrence. *AVN Bulletin*. No. 1 (26).

Chekinov, S., Bogdanov, S. (2011). The Influence of Indirect Actions on the Character of Modern Warfare, *Voennaya Mysl'* no. 6.

Chekinov, S., Bogdanov, S. (2013). The Nature and Content of a New-Generation War. *Military thought*, October - December 2013.

Chekinov, S., Bogdanov, S. (2017). Evolution of the Essence and Content of the Concept of "War" in the 21st Century. *Military Thought*, January 2017, Retrived from January 23, 2024, from <https://dlib.eastview.com/browse/doc/50724910>.

Chekinov, S. Bogdanov, S. (2010). Asymmetrical Actions to Maintain Russia's

Military Security, *Voyennaya Mysl'*, No. 3.

Chekinov, S. Bogdanov, S. (2013). O Kharaktere i Soderzhanii Voiny Novogo Pokoleniya. *Voennaya Mysl'*, No. 10.

Clark, M. (2020). *Russian hybrid warfare*. Institute for the Study of War, Military learning and the future of war series, September 2020.

Cordey, S. (2019). Cyber Influence Operations: An Overview and Comparative Analysis. *ETHZ Research Collection*. <https://www.research-collection.ethz.ch/>

Doktrina Vojske Srbije. *Službeni Vojni list RS*. br. 2/ 2010.

Dulnev, P. Litvinenko, V. (2016) With Accumulated Experience – Into the Future. *Army Collection*, January 2016.

Ehlers, R. (2017, January 3). *Making Old Things New Again: Strategy, the Information Environment, and National Security*. The Strategy Bridge. Retrived from March 23, 2024, from <https://thestrategybridge.org/>.

Gareev, M. (2009). Strategicheskoe sderzhivanie – vazhneishee napravelnie natsional'noi bezopasnosti, *Stratgicheskaiia Stabil'nost'*, no. 1.

Gerasimov, V. V. (2013). The Value of Science is Foresight, *Voенно-promyshlennyi kur'er*, Feb. 26, Retrived from January 23, 2024, from <https://vpk-news.ru/articles/14632>.

Gerasimov, V. V. (2013). Basic trends in the development of forms and methods of using the Armed Forces, current tasks of military science for their improvement, *Vestnik*, AVN, no. 1 Retrived from January 23, 2024, from <http://www.avnrf.ru/index.php/zhurnal-qvoennyj-vestnikq/arkhiv-nomerov/534-vestnik-avn-1-2013>.

Ignatius, D. (2022). Watching Russia's military failures is exhilarating. But a cornered Putin is dangerous., *The Washington Post*, March 17, 2022, Retrived from January 23, 2024, from <https://www.washingtonpost.com/opinions/2022/03/17/cornered-putin-dangerous-ukraine-david-ignatius/>;

Kofman, M. Fink, A, Edmonds, J. (2020). *Russian Strategy for Escalation Management: Evolution of Key Concepts*, April 2020, CNA, CNA's Strategy, Policy, Plans, and Programs Division (SP3).

Kondakov, E. E. (2022). Nonmilitary measures of ensuring the military security of the Russian Federation and the main problems of their implementation, *Flot.com*, Retrived from January 20, 2024, from <https://flot.com/publications/books/self/safety/11.htm>.

Manoilo, A. (2004). Upravljenje psihologicheskoj voinoi v sisteme informacionnoi gosudarstvennoi politiki. *Politika i Obschestvo*, no. 2, 2004.

Miljković, M. Jevtić, D. (2021). Sukobi u informacionom prostoru iz ugla savremene vojne misli u Ruskoj Federaciji – iskustva za bezbednost Republike Srbije, *Nacionalni interes*, Godina XVII, vol. 40 Broj 2/2021.

Miljković, M., Jevtić, D. (2021). Sukobi u informacionom prostoru iz ugla savremene vojne misli u Ruskoj Federaciji – iskustva za bezbednost Republike Srbije. *Nacionalni interes*, 2021/2, 107.

Modestov, S.A. (1998). *Informacionnoe protivoborstvo kak faktor geopoliticheskoy konkurencii*. M.: Izdatel'skiy centr uchebnyh i nauchnyh programm.

Modestov, S.A. (2009). Strategic deterrence in the theater of information warfare. *Strategic Stability*, no. 1.

Nezhdanov, I. (2016). *Technologies of information wars on the Internet*, Our youth Retrived from January 23, 2024, from <https://studylib.ru/doc/2333221>

Obrashchenie Prezidenta Rossiiskoi Federatsii, (2022, February 24,), *Kremlin.ru* <http://kremlin.ru/events/president/news/67843>.

Paparin, I. (2012): *Doktrina informacione odbrane Rusije*, Beograd: Evroazija.

Paybarah, A. (2022). A Kremlin Spokesman Says Russia Could Use Nuclear Weapons If There Is 'An Existential Threat For Our Country, *The New York Times*, March 23, <https://www.nytimes.com/2022/03/22/world/europe/russia-nuclear-weapons-cnn.html>.

Pechurov, S. Alexander, S. (2017). Lessons from Coalition Wars in Interpreting Western Military Theory. *Military Thought*, April.

Roldugin, D. Kolod'ko Yu.V. (2015). A clarification of the concept of deterrent damage in resolving the tasks of deterrence through the use of force. *Strategic Stability*, no. 4.

Roth, A., Connolly, K. Raskin, J. (2022). Vladimir Putin Puts Russia's Nuclear Deterrence Forces On High Alert. *Sputniknews*. <https://sputniknews.com/russian-special-military-op-in-ukraine/>, February 27, 2022.

Russia Threatens to Deploy Tactical Nuclear Weapons. (2024, Januar 23). *VOAnews.com* <https://www.voanews.com>

Sharikov, P. (2013). V Boi Idut Kibervoiska, *NVO*, 13 April 2013.

Thomas, L. T. (1996). Russian Views on Information-based Warfare. *Airpower Journal*, Special Edition.

*Hatidža Beriša*¹
*Dejan Petrović*²
*Milan Miljković*³

CHANGE OF MILITARY DOCTRINES IN THE RUSSIAN-UKRAINIAN WAR AS A FACTOR OF NEW TECHNOLOGIES⁴

Abstract

The topic of the paper is the perception of war as a product of political conflict, with the application of new modern technology, which is available to the opposing sides. History is full of numerous examples of underestimating technology. It is enough to look at the example of Israel, which won many wars against Arab countries by applying advanced technology. Technology continues to develop unstoppably, and humanity and civilizations have no choice but to constantly get used to new information and technological changes. Among those who should be the first to monitor and adapt to such changes are decision-makers, that is, military leaders (commanders), because these changes first occur in the environment itself, which is constantly changing. As a result, the process of technology is being improved, and the introduction of new technologies is becoming inevitable. Automation, computerization and robotization are becoming the main trend in the development of modern weapons. The aim of the paper is to examine how new technologies have influenced changes in the military doctrines of the Russian Federation (RF) and Ukraine during the current conflict, with the focus on determining whether new technologies have led to a key advantage for one of the warring parties that changed its doctrine faster. The research used the method of content analysis that discusses the rapid development of technology, which has gained a new dimension in this war. Methods of analysis and deduction have been used to consider how and in what way new technologies have influenced certain changes in doctrines on both sides.

Keywords: *doctrine, defense, technology, changes, Russian Federation, Ukraine.*

¹ School of National Defense, University of Defense in Belgrade, Serbia, berisahatidza@gmail.com

² School of National Defense, University of Defense in Belgrade, Serbia

³ School of National Defense, University of Defense in Belgrade, Serbia

⁴ The paper is part of a scientific project of the National Defense School "Vojvoda Radomir Putnik" of the Defense University of the Ministry of Defense, entitled "Neutrality and Strategic Deterrence", project number: ŠNO-DH/1/2224

DOCTRINES OF OPPOSING PARTIES IN UKRAINE

Doctrinal inadequacy is no less a common cause of defeat or unnecessary reversal than technological obsolescence.

Colin S. Gray

Changes in military doctrines are a continuous, evolutionary process that takes place in almost all countries of the world. What is doctrine? In the most general sense, doctrine is an approved document that teaches, either through school or in an operational unit through training, what methods to use to achieve a military objective. Doctrine finds its origins in previous experiences, that is, it reflects the official acceptance of best practices that have been repeatedly applied in the past. From the above it follows that doctrine has two basic purposes. First, it provides guidance to decision makers and planners who develop plans and policies, how to act in certain situations and similar contexts. Second, it provides formal knowledge that ensures a common level of understanding and solving problems, either existing or that may arise. From the above it follows that doctrine is, on the one hand, an accumulation of scientific knowledge and, on the other hand, a system of statements of views with a distinctly paradigmatic value. Military doctrines, in a general sense, can be offensive, defensive and deterrent. For a simpler understanding of the above definition of military doctrines, one can see how the Russian Federation and Ukraine established their doctrines before the start of the war on February 24, 2022.

Russian Federation

Since the collapse of the Soviet Union, the Russian Federation has invested serious efforts in reform processes in order to create and transform the Russian Armed Forces into one of the strongest military powers in the world. This was not an easy process, because on the one hand, given the fact that there were high expectations both externally and internally that the Russian Federation possessed a traditionally powerful military force, and on the other hand, there were numerous problems in Russian society, inherited from the times of the USSR. The reform of Russian society as a whole was based on the geopolitical premise that the Russian Federation is a great power that can independently project its geopolitical interests. In this regard, during the last decade of the last century, and especially after Vladimir Putin came to power in the Russian Federation, a process of significant reform of the Russian army began. During that period, the Russian Federation faced serious challenges in Chechnya, especially in the first war with Chechen rebels. That conflict raised alarm bells in Russian society, leading to a general climate of necessity for investments and changes in the Russian military. During that period, significant progress was recorded, primarily in the status of military per-

sonnel, but also in the improvement of the general situation in the military.⁵

The Russian military has sought to prepare for and wage potential wars in accordance with the "Deep Battle" doctrine, which envisages fighting at any level of warfare. Positive developments in the Russian military were best seen in the short Russian-Georgian conflict in 2008. Although Georgia was defeated relatively quickly, that conflict, in addition to its success, also revealed certain problems in the Russian military. The most noticeable problem that the Russian military faced in that conflict was outdated, inadequate weapons and insufficient training of soldiers to handle modern weapons. In order to overcome this problem, President Dmitry Medvedev, in his ten-year projection of the military budget for the period 2010-2020, has foreseen about 425 billion US dollars for the modernization of weapons, logistical support, intelligence technologies and similar needs. In addition, at the initiative of the President of the Russian Federation, a new reform of the Russian army was initiated. This was followed by a new military doctrine, which was signed by the Russian President in February 2010, although the process of its preparation began in 2005.

As a result of the new doctrine, after the aforementioned conflict, the Russian army abandoned the regimental-division structures, as they proved to be outdated, and switched to a more flexible brigade organization that is linked to operational-tactical commands, and those to military districts. In addition, the reform also included human resources and a significant reduction in the number of troops in the Russian Federation was initiated, with the aim of creating smaller, but functionally capable armed forces.

The improvement of the situation in the Russian army was further helped by participation in the war in Syria. Namely, at the invitation of Syria, the Russian Federation sent part of its forces, formed bases and was a decisive factor, along with Iran, in saving Syria from complete collapse. The aforementioned experiences, both in land and air operations, influenced the additional strengthening of the Russian army. Therefore, the war in Syria can be considered an "exercise" for the Russian Federation's operations in Ukraine, which began in February 2022.

During the war in Ukraine, the Russian army initially sought to quickly seize key cities, including Kyiv, through deep airborne penetrations and attacks from multiple directions, thereby breaking the Ukrainian will to fight. However, the results were not as expected, although a large part of Ukraine's territory was occupied. Namely, the Russian army suffered significant losses in manpower and equipment, and had no answer to some of the new Ukrainian assets, such as unmanned aerial vehicles. This led to a change in strategy. A strategy of attrition was adopted, the remobilization of personnel, which was significantly lacking in the first months of the war, was carried out, and active defense was adopted on most of the battlefield.

⁵ The authors, based on analysis during the execution of exercises with participants at the General Staff training, came to their views, so the work is based exclusively on knowledge and monitoring of discussions and polemics during the implementation of the teaching.

Ukraine

After gaining independence, Ukraine struggled for years with internal disagreements and frictions over whether to align with the East or the West, the Eastern or Western bloc. This was reflected in the Ukrainian armed forces, which in the early years relied on weapons, equipment and doctrine inherited from the USSR. However, after 2013 and the takeover of power by pro-Western politicians, the process of adapting to Western doctrines began. This was also contributed to by the war with pro-Russian rebels in 2014. The above experiences, along with Western mentorship, significantly increased the operational readiness of Ukrainian armed forces. In the period 2014-2023, Ukraine essentially adopted Western military doctrines and, through almost continuous combat operations on the lines of demarcation with the rebels, rotated the best forces and trained them. ⁶ During that period, Ukraine prepared its military forces to crush the rebel forces in eastern Ukraine. They were trained by American instructors in accordance with the doctrine of "*Air-Ground Battle*" in order to break the resistance of the rebels through joint operations, with the support of the allies. However, the Russian Federation was the first to launch an attack on Ukraine, which led to a war that has entered its third year.

How did Ukraine stand up to the militarily superior Russian army? First of all, the good training that the Ukrainian army received from the US. Second, the enormous intelligence support that they continuously receive from the US and Great Britain. Third, the experience they gained in operations against the rebels in the East. Fourth, and probably most importantly, the doctrine that they adopted during training with members of the US Armed Forces. Namely, Ukraine adopted a doctrine of fighting a powerful enemy such as the Russian Federation. The doctrine also included resistance forces that they hid among the civilian population. Ukraine developed a doctrinal approach that included military and non-military resistance to the enemy. In addition, they have very successfully combined cheap, civilian technologies with military donations from the West, and have struck at the Russian military in unexpected ways.

NEW TECHNOLOGIES IN THE RUSSO-UKRAINIAN WAR

Technology has always been used to produce improved weapons of war. In the modern era, which is generally considered to have begun after the French Revolution, systematic research in science has enabled the development of new technology and innovations for military and civilian use. This has had an impact on both society and the nature of warfare. Modern Russian military theory recognizes six, or seven, generations of war. First-generation wars used blades, bows, and crossbows. Second-generation

⁶ This would have significant results in overcoming the first days of the war and would be exploited through successful actions on the flanks and logistics of the Russian army, which was very stretched.

wars used smoothbore weapons. Third-generation warfare was dominated by rifles. Fourth-generation wars are dominated by tanks and aircraft, while fifth-generation is expected to be dominated by nuclear weapons. Sixth-generation wars are dominated by long-range precision weapons. Seventh generation wars will bring the destruction of computer databases and hacker attacks of all kinds.

Over the past few years, the trend of introducing various technologies for military purposes has continued. Some of these technologies have already been seen in the previous two decades, but significant modifications have been made in the meantime, and they can be seen as new tools. The most obvious example is drones, which in just a couple of decades have gone from being tools intended for collecting intelligence from the airspace to becoming one of the most deadly tools in the war in Ukraine.

Expectations that technologies will become available to all states are proving to be unrealistic. It is necessary to accept that economic power and technology are directly correlated. Economic power is determined by technological development and as such translates into military power. Therefore, it is not surprising that the use of new technologies can be observed in the war in Ukraine, as it is a conflict in which the military powers of the East and the West are opposed.

New technologies that have been applied in the Russian-Ukrainian war indicate the increasing importance of artificial intelligence. Namely, artificial intelligence has significantly improved the command and control system in combination with means that enable visualization of the battlefield.⁷ This allows for coordination and improvement of individual and collective capabilities of units directly on the ground. In addition, the introduction of artificial intelligence in systems used by commanders allows for faster decision-making and more precise calculation of the advantages and disadvantages of certain variants of use (strategic and operational levels). At the tactical level, the use of artificial intelligence allows for faster coordination of soldiers and autonomous platforms, which contributes to increasing the efficiency and effectiveness of combat operations. The possibility of monitoring operations via video transmission creates a direct possibility of coordinating the strategic and tactical levels because the process of making a decision and its execution on the ground is shortened.

High-precision long-range weapons represent one of the most significant technological achievements, dating back to the last century, especially since continuous modernization and creation of more powerful systems are being carried out. The war in Ukraine has seen, especially in the first months, the massive use of various types of long-range weapons, including the most modern hypersonic missiles "Kinzhal", which have great destructive power and speed, as well as the ability to maneuver along the entire flight path to the target. These weapons have been announced as one of the most

⁷ Although video transmission using drones has previously been used by US forces in Afghanistan, Pakistan and other countries, the war in Ukraine has led to the massive use of these technologies by both sides.

promising weapons at the disposal of the Russian Federation. Although the results of the use of these missiles are still contradictory, further use of these weapons can be expected. In addition to the above missiles, the capabilities of missile systems have been improved, such as the Ukrainian anti-ship missiles "Neptune". The use of these missiles, in coordination with US intelligence capabilities, has led to significant successes for the Ukrainian Navy in combat with one of the most powerful fleets in the world, the Russian Black Sea Fleet. High-precision weapons are also widely used in urban operations to avoid major collateral damage.

In the war in Ukraine, it can be stated that military operations are undergoing a multiplication of power through the use of unmanned platforms of all kinds. The complexity of modern military operations indicates the necessity of a high level of intelligence activities in all phases of operations. Therefore, means are necessary that can approach unnoticed, collect intelligence on the activities of the opposing side in order to detect all activities and create a clear picture of their intentions, composition, numbers, hiding places, weapons depots, etc. This is precisely where the need for modern optoelectronic means, such as drones, is seen, because they enable monitoring of the enemy even in the most complex circumstances, such as urban environments in which it is difficult to distinguish soldiers from civilians. This is especially important due to the fact that occasionally, in combat operations, women, children and the elderly are massively abused in order to gain support from the wider international community.

Information warfare and the use of cyber technologies in Ukraine have been applied by both warring parties, but the effects can be assessed as secondary to the effects of kinetic weapons, so for now the hypothesis that they retain their importance as auxiliary components of military operations is confirmed.

In addition to the above technologies, it is worth mentioning that Ukraine is also massively implementing new technologies in the field of air defense (AD). Although there is not enough data on how to counter the massive use of drones on both sides, it is noticeable that Russian air defense systems, in combination with the latest electronic warfare systems, are successfully eliminating the use of these means, even though they are among the newer technologies. There are also ongoing announcements that the Russian Federation could also use the latest S-500 air defense system, which should be able to shoot down even the most advanced systems in the world.

When considering new technologies being applied in the current war, one cannot ignore the advanced and modernized use of artillery systems and guided ammunition based on elements of unmanned platforms with built-in artificial intelligence. The use of all artillery systems in combination with guidance by unmanned aerial vehicles is one of the most important characteristics of success in operations in Ukraine, especially by the Russian army, which has a huge arsenal of these weapons at its disposal.

The aforementioned new and modernized technologies brought great advantages to the parties using them in the war in Ukraine. They once again confirmed that technology is a vector of change in the use of forces.

NEW TECHNOLOGIES AND CHANGES IN MILITARY DOCTRINES IN THE RUSSIAN-UKRAINIAN WAR

The difference in power between the Russian and Ukrainian forces is enormous. First of all, Russia is a nuclear power, and Ukraine renounced that status after independence. Therefore, it is impossible to wage a "fifth generation" war. However, the question is how profitable it is for the Russian Federation to wage a "sixth generation" war, given the limited number of precision, long-range weapons. In the first months of the war, applying the "Defense in Depth" doctrine, the Russian army launched a significant part of the stock of such weapons and thereby exhausted significant reserves. Therefore, the Russian army, considering that it did not achieve the desired effects, sought to change the doctrine on the fly, among other things, due to the use of new technologies that Ukraine received from its allies. A similar case occurred with Ukraine, which had to partially change its "Air-Ground Battle" doctrine, which it had taken over from the US, because it could not withstand the massive artillery and missile strikes of the Russian army.

The use of new technologies in the war in Ukraine led to changes in the doctrines of the opposing sides, although these changes were not immediately implemented. They could be observed during the analysis of publicly available information that followed the events on the ground. The secrecy of the changes in doctrine was expected because these changes sought to neutralize the advantage that the technology brought to one side or the other.

The massive use of artificial intelligence and battlefield visualization allowed both sides to accelerate the flow of information and flexibly command their forces, although not in all phases of the war. This especially applies to the Russian army, which suffered significant losses in the first months of the war because the information transmission system was damaged or interrupted due to the actions of the Ukrainian army and the weak sustainability of the Russian forces. In order to adapt to the new situation, the Russian forces had to make certain changes to the doctrine of the use of operational formations, that is, the flow of information and operations accelerated, all as a result of the use of new technologies by the Ukrainian army. Namely, the Ukrainian army used the Starlink space orbital information network (SpaceX's StarLink). In addition, both sides adjusted their doctrines regarding the conduct of information operations and the use of cyber weapons. The general opinion is that the Russian Federation, before and after February 24, 2022, failed to achieve information superiority over the adversary, which negatively affected the effectiveness of the implementation of information-based deterrence measures. Conflict and deterrence in the information space in this conflict were conducted

through operations in cyberspace, in the propaganda and intelligence areas, as well as through competition in the area of mastering the adversary's communication systems. The preliminary conclusion is that the Russian side was expected to achieve much more results in terms of deceiving the adversary, cyber operations, propaganda activities in the area of strategic communication, or influencing the adversary's communication on the battlefield, which is placed at the top of the list of goals in Russian military theory and deterrence doctrine. International military experts were surprised by the fact that at the beginning of hostilities, from February 24, 2022, the Russian Federation did not launch a cyber attack on the Ukrainian telecommunications infrastructure. Ukraine remained online throughout the special military operation, although Russian military doctrine implies the use of cyber effects in addition to traditional kinetic warfare. There is evidence that Russia tried to cause cyber effects on the Ukrainian internet network, but they were reduced by the new connection via Starlink.

The use of unmanned aerial vehicles, first by the Ukrainian armed forces, and then by the Russians, has led to a change in the use of forces in operations. Numerous successful examples of combining UAVs with other types of weapons have been observed, which has led to the maximization of the effects of fire and maneuver. This has led to the need to abandon any grouping of forces at all costs, to a scattered deployment of units and assets, the mandatory use of camouflage of movements and assets in order not to be detected from the airspace, a significant use of forces for electronic warfare, as well as air defense. All this has led to doctrinal changes in the use of forces, because large-scale military operations cannot be carried out in classical ways, by grouping large forces in certain directions, especially if the enemy has powerful artillery and missile systems that are linked to the above-mentioned observation systems.

The use of the promising Kinzhal system by the Russian army has influenced the change in the air defense doctrine of the Ukrainian army. Considering that they did not have the most modern means or the doctrine of the use of such means, the most modern air defense means and systems were purchased through donations. In addition, early warning systems were purchased, so that layered air defense could be activated in a timely manner to protect critical infrastructure. Currently, there is not enough data on the effectiveness of defense against this promising means of the Russian army, but significant results have been achieved in the fight against air defense and cruise missiles. Therefore, among other things, the Russian army has partially changed the doctrine of the use of air forces. Namely, there have been numerous cases of first launching cheap drones of Iranian origin at Ukrainian targets in order to jam the enemy's air defense, and then launching high-precision missiles and guided bombs. According to unconfirmed information, one of the Ukrainian Patriot air defense systems was also damaged in this way. However, thanks to numerous donations of various air defense systems, the Ukrainian army prevented the complete supremacy of the Russian army in the air, which

led to a change in the doctrine of the use of aircraft that had to operate from long distances, which significantly facilitated the defense of Ukraine.

The use of new long-range, high-precision weapons has significantly influenced the doctrine of the use of forces. One example is the use of Ukrainian land-to-sea missile systems⁸, which led to a partial change in the doctrine of the Russian naval forces. This was particularly influenced by the sinking of the cruiser "Moskva", which was the command ship of the Black Sea Fleet, and was also intended for the electronic protection of the fleet. Therefore, the ships had to move significantly away from the coast and organize themselves in a different way in order to still carry out the mission of the naval blockade of Ukraine.

The advanced artillery systems of the Russian Federation, in combination with precision-guided munitions, have created major problems for the Ukrainian army, especially in conducting offensive operations. This led to a change in doctrine in conducting the counteroffensive, i.e. attacks were carried out with small, highly mobile forces in order to avoid high casualties while passing through the system of obstacles set up by Russian forces. It is believed that this is one of the reasons why the counteroffensive failed, although it was accompanied by high casualties among the Ukrainian army.

Given that the current conflict in Ukraine is still ongoing, it can be considered that the list of new technologies that have been used is not yet final. However, based on the examples presented, it is obvious that the warring parties must quickly adapt to changes on the front and change and adjust the doctrines of the use of armed forces. The rapid change of the situation on the ground makes it impossible to change doctrines in the usual way as in peacetime. On the contrary, most changes occur unannounced, secretly, and all with the aim of achieving strategic surprise.

CONCLUSION

Modern armies are constantly striving for continuous development and integration of new capabilities, in accordance with changes in the conflict paradigm. The modern era can be characterized as a period of knowledge, high-tech and, above all, non-linear conflicts. Today's wars, as seen in the Armenian-Azerbaijani and especially the Russian-Ukrainian wars, are characterized by all three forms of conflict: conventional, asymmetric and hybrid. They differ from previous ones, qualitatively and quantitatively, because technology and war have become allies. New technologies have significantly influenced the shaping of conflicts, as well as the battlefield itself.

Rapid changes in military technology, as can be seen in the war in Ukraine, have led to the development of new high-precision weapon platforms that can deliver a large amount of kinetic energy to the target. There are also unmanned systems armed with high-precision ammunition, homing ammunition guided by artificial intelligence, a new

⁸ Ukrainian-made missile "Neptune".

generation of artillery missiles for precision shooting at very long distances, and many other high-tech systems. All of them affect the change in military doctrine and the methods of conducting military operations.

Experience from the war in Ukraine indicates that both sides are trying to use as many new technologies as possible in order to gain an advantage in operations. This, on the one hand, has initiated the need to revise doctrinal documents and foresee doctrinal, operational-tactical and technical measures that will enable the armed forces to use new technologies in the most effective way. On the other hand, doctrinal changes allowed for defense against the other side using weapons and equipment enriched with new technologies that maximized the effectiveness of existing assets.

Although new technologies caused changes in the military doctrines of the warring parties, they still did not bring a key advantage for winning the war. One of the reasons is the fact that the states that are at war have great human and material potential and can afford significant losses and continue military operations without hindrance. However, the side that is able to use more advanced technologies, and is more adaptable to changes and is also able to change the doctrine of use faster, will win the war.

*Miranda Gurgenidze*¹
*Tamazi Urtmelidze*²

INTELLECTUAL PROPERTY IN GLOBAL SECURITY: BALANCING RIGHTS AND PROTECTION STRATEGIES

Abstract

This study explores the critical intersection of Intellectual Property (IP) rights and global security, highlighting the dual nature of IP laws as both catalysts for economic growth and innovation, and potential sources of conflict and insecurity. It underscores the importance of strong IP laws for economic stability and innovation, which are vital for maintaining global security while acknowledging the challenges in enforcing these laws across different jurisdictions. The paper aims to closely examine the impact of IP on global security, investigating how the protection and enforcement of IP rights affect, and how they are influenced by international security dynamics. It considers IP laws as tools that can foster economic development and technological advancement, contributing to a more stable global environment, but also as potential triggers for disputes and insecurity due to misuse or inconsistent enforcement. Through qualitative research, including analysis of international agreements, national legislation, and case studies, the study provides insight into the complex role of IP rights in the global security landscape. It addresses the benefits of IP protection for fostering innovation and economic growth, alongside the security challenges posed by counterfeiting, piracy, and cyber threats. The research highlights the inconsistency in international IP law enforcement as a significant issue. Concluding, the paper advocates for a balanced approach to IP law, emphasizing the need for international cooperation and legal harmonization to reconcile economic incentives with global security needs. It calls for adaptable and responsive IP policies considering the rapidly evolving technological domain, contributing to a broader understanding of the nexus between IP law and global security.

Keywords: *Intellectual Property (IP), global security, economic stability, technological innovation legal harmonization.*

¹ Law and International Relations Faculty, Georgian Technical University, Tbilisi, Georgia,
Gurgenidzemiranda07@gtu.ge

² Georgian Technical University, Tbilisi, Georgia

INTRODUCTION

Intellectual Property (IP) is defined by the World Intellectual Property Organization (WIPO) as creations of the mind, such as inventions, literary and artistic works, designs, and symbols, names, and images used in commerce. IP is legally protected through patents, copyright, trademarks, and more, enabling creators to gain recognition or financial benefits from their innovations. This system aims to foster an environment where creativity and innovation can thrive, balancing the interests of innovators and the public (World Intellectual Property Organization, n.d.). This essay discusses the significance of strong IP laws for economic stability and innovation, crucial for global security, while acknowledging the challenges in enforcing these laws across jurisdictions. The study aims to examine the impact of IP on global security by investigating how the protection and enforcement of IP rights affect, and are influenced by, international security dynamics. It considers IP laws as instruments that can foster economic development and technological advancement, contributing to a more stable global environment, but also as potential triggers for disputes and insecurity due to misuse or inconsistent enforcement. Through qualitative research, including analysis of international agreements, national legislation, and case studies, the paper provides insights into IP rights' complex role in the global security landscape, highlighting the benefits of IP protection for innovation and economic growth alongside the security challenges posed by counterfeiting, piracy, and cyber threats. It concludes with a call for a balanced approach to IP law, emphasizing international cooperation and legal harmonization to reconcile economic incentives with global security needs, advocating for adaptable and responsive IP policies in the rapidly evolving technological domain.

Methodology

The paper employs a qualitative research approach, drawing on various sources including international agreements, national laws, and existing literature on IP rights. Through detailed examination and case studies, it explores how IP rights intersect with, contribute to, and influence global security dynamics.

Results

The analysis reveals a dual nature of IP laws. On one hand, they significantly contribute to economic growth and technological advancement, acting as catalysts for economic stability and global competitiveness. On the other, they pose notable challenges to global security, especially concerning counterfeiting, piracy, and cybersecurity threats. The paper discusses the importance of robust IP frameworks for national competitiveness and economic security, highlighting the correlation between strong IP protections and

economic performance. Conversely, IP infringement risks such as trade secrets theft and counterfeit production are scrutinized for their negative impact on economic security.

Intellectual property by itself neither helps nor hinders development necessarily. It is how laws, policies and practices are designed and used in different countries that determine whether IP is effective for development purposes. Flexibilities in the international treaties and agreements can facilitate development because countries can use them in a manner that enables them to pursue their own public policies, either in specific fields like access to pharmaceutical products (for instance, through compulsory licensing in some circumstances) or protection of their biodiversity (with patents or another unique system), or more generally, in establishing macro and microeconomic and institutional conditions that support development. Intellectual property is a foundational element of the global economy, driving innovation, economic growth, and cultural diversity. Effective IP protection strategies are essential for maintaining the balance between encouraging creativity and innovation and ensuring that the benefits of creations are accessible to society at large. Economic security is intricately linked to the protection and management of Intellectual Property (IP). A robust IP framework is not only a catalyst for innovation and economic growth but also a cornerstone for national competitiveness in the global market. This discussion delves into how IP influences economic security, the benefits of strong IP protection, and the risks associated with IP infringement (United States Patent and Trademark Office, n.d.). Economic stability and security are bolstered by the positive correlation between strong IP protections and economic performance. IP-intensive industries often contribute significantly to a country's GDP, employment, and trade balance. For instance, industries that rely heavily on patents and copyrights, such as the software, entertainment, and biotech sectors, not only generate high-paying jobs but also drive export growth, thereby enhancing economic resilience (United States Patent and Trademark Office, n.d.).

Conversely, the theft of IP, including trade secrets theft and the production and distribution of counterfeit goods, poses significant risks to economic security. IP infringement can lead to: **Loss of Revenue:** Companies victimized by IP theft lose revenue to counterfeiters and unauthorized users of their technology, impacting their profitability and sustainability; **Erosion of Competitive Advantage:** The unauthorized use or imitation of patented technologies or creative works can erode a firm's competitive edge, diminishing its market share and weakening its position in both domestic and international markets; **Undermining Innovation:** If IP rights are not effectively protected and enforced, businesses and individuals may be discouraged from investing in new innovations, knowing that their efforts and financial investments could be easily appropriated by others without proper compensation. To mitigate these risks, it is crucial for countries to not only establish comprehensive IP laws but also ensure their rigorous enforcement. Effective enforcement mechanisms, including border controls to prevent the importation of counterfeit goods and legal remedies for IP infringement, are essential. Additionally, international coopera-

tion plays a pivotal role in combating IP theft, given the global nature of markets and the cross-border challenges of enforcing IP rights. Collaboration through international treaties and agreements, such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the Anti-Counterfeiting Trade Agreement (ACTA), helps harmonize IP laws across countries and sets a global standard for protection and enforcement.

In an era where technological advancements play a pivotal role in national defense, economic stability, and cyber operations, the management and protection of IP emerge as key factors influencing global security dynamics. By examining the implications of IP in areas such as: Technology transfer, cybersecurity, and defense innovation, this part of the article aims to provide insights into how robust IP frameworks can contribute to enhancing global security. The concept of technology transfer, particularly when it involves dual-use technologies, occupies a critical nexus between innovation, economic development, and global security (World Intellectual Property Organization, n.d.). Dual-use technologies, characterized by their potential application in both civilian and military contexts, present unique challenges and opportunities for the international community. Intellectual Property (IP) rights play a pivotal role in managing these challenges, regulating the flow of technology across borders, and mitigating security risks while fostering global innovation and collaboration (Falvey & Foster-McGregor, 2006). Dual-use technologies, ranging from artificial intelligence (AI) and biotechnology to quantum computing and cybernetics, are driving the next wave of technological advancement. While these technologies promise significant benefits for societal progress, healthcare, and the environment, they also pose potential risks if misused or if they fall into the wrong hands. The proliferation of such technologies can lead to an escalation in arms races, enable the development of unconventional weapons, or enhance the capabilities of non-state actors and rogue nations in conducting cyber warfare, bio-terrorism, or other forms of asymmetric warfare (Wassenaar Arrangement Secretariat, n.d.). However, the protection offered by IP rights also necessitates a careful balance. Excessive restrictions on technology transfer can hinder global scientific progress and cooperation, limiting the development and deployment of beneficial technologies. Conversely, lax IP protections may facilitate the unregulated spread of dual-use technologies, increasing proliferation risks. Effective management of dual-use technologies through IP rights requires a multi-faceted approach:

International Collaboration: Countries need to work together to establish common standards for the protection and transfer of dual-use technologies. International treaties and agreements, such as the Wassenaar Arrangement, play a crucial role in setting export controls and licensing requirements for sensitive technologies (Wassenaar Arrangement Secretariat, n.d.).

Clear and Consistent IP Policies: Nations should develop clear and consistent IP policies that address the challenges of dual-use technology transfer. This includes

defining what constitutes a dual-use technology, setting guidelines for patent disclosures that might have security implications, and establishing protocols for international cooperation in IP enforcement.

Public-Private Partnerships: Collaboration between governments and the private sector is essential for balancing innovation with security. Companies involved in the development of dual-use technologies must be active participants in national and international discussions on IP rights and security, ensuring that their innovations do not inadvertently compromise global security.

Research and Education: Investing in research to understand the security implications of emerging technologies and educating innovators about the potential dual-use applications of their work can help mitigate risks. Awareness programs can equip scientists and engineers with the knowledge to navigate the complex landscape of IP rights and security considerations.

The ultimate goal of regulating technology transfer through IP rights is to ensure that advancements in dual-use technologies contribute positively to global security. This involves leveraging these technologies to enhance defense capabilities, improve intelligence and surveillance for crime prevention and counter-terrorism, and foster international cooperation in addressing global challenges (World Intellectual Property Organization, n.d.). By carefully managing the dissemination of dual-use technologies, the international community can harness their potential for good while minimizing the risks they pose to global security. So, the intersection of technology transfer, IP rights, and global security is a dynamic and complex field. As dual-use technologies continue to evolve, so too must the strategies for their regulation. Through international collaboration, robust IP frameworks, and a commitment to ethical innovation, it is possible to navigate the dual-use dilemma and ensure that technology transfer advances global security objectives. In the rapidly evolving digital landscape, cybersecurity emerges as a critical shield against a spectrum of threats that endanger not just individual privacy but also national and global security. Intellectual Property (IP) rights are integral to this defense, providing a legal framework that protects the fruits of innovation in the cyber domain. The digital economy is underpinned by software, databases, and various forms of digital content, all of which are susceptible to piracy, unauthorized use, and theft. IP rights, particularly copyrights and patents, offer protection to these digital assets, ensuring that creators and innovators can control how their works are used and distributed. This legal protection is crucial for fostering a secure environment where innovation thrives, incentivizing the development of new technologies and solutions that enhance cybersecurity. In major legal systems software, the backbone of digital systems, is protected under copyright law, which prevents unauthorized copying, modification, or distribution. In some countries patents can also protect unique software algorithms and functionalities, offering another layer of security against infringement and ensuring that innovative cy-

bersecurity solutions are commercially viable. Databases containing sensitive personal or business information are protected under copyright and *sui generis* database rights (in certain jurisdictions), safeguarding against illicit extraction and use of data (European Parliament and Council, 1996). This protection is vital for maintaining the confidentiality and integrity of data that could be exploited if fallen into the wrong hands. The robustness of digital infrastructure, including networks, servers, and communication systems, is paramount for national security and economic stability. IP rights play a pivotal role in securing this infrastructure by encouraging the development and deployment of advanced cybersecurity technologies. Patents incentivize R&D in cybersecurity, leading to the creation of innovative security solutions such as firewalls, encryption technologies, intrusion detection systems, and malware protection tools. These technologies are essential for defending digital infrastructure against increasingly sophisticated cyber threats. Standard-Setting and Interoperability: IP rights also contribute to the establishment of security standards and protocols that ensure interoperability and reliability across different systems and technologies. By protecting the proprietary technologies that underpin these standards, IP rights support a secure and cohesive digital environment. The resilience of cyber systems against attacks and breaches is critical for minimizing the impact of cyber incidents and ensuring rapid recovery. IP rights contribute to this resilience by facilitating the development and dissemination of robust cybersecurity measures. While IP rights are instrumental in enhancing cybersecurity, they also present challenges, such as impeding the free flow of information critical for collaborative cybersecurity efforts due to their exclusivity. Balancing IP protection with the need for openness in sharing cyber defense strategies is complex. Additionally, the global nature of cyber threats demands international cooperation to harmonize IP laws and enforcement strategies, which can be difficult due to varying national legal frameworks and interests. This necessitates careful management to ensure that IP rights support, rather than hinder, global cybersecurity resilience. Balancing the openness necessary for collaborative security efforts with the exclusivity granted by IP rights requires careful consideration.

Furthermore, the global nature of cyber threats calls for international cooperation in harmonizing IP protections and enforcement to effectively combat cybercrime and protect digital innovations. As the digital realm continues to expand, the intersection of cybersecurity and IP rights becomes increasingly critical. IP protections are vital for fostering innovation, securing digital infrastructure, and enhancing the resilience of cyber systems (Jackson, 2024). By ensuring that digital innovations receive the legal protection they deserve, IP rights not only safeguard the economic interests of creators and businesses but also fortify the digital frontier against the myriad of cyber threats that challenge national and global security. In navigating the complexities of the digital age, a nuanced understanding of the symbiotic relationship between cybersecurity and IP rights is essential for crafting policies and strategies that protect and propel the digital

economy forward. The interplay between defense innovation and intellectual property (IP) rights is a cornerstone of contemporary national security and military advancement. IP rights, especially patents, are the bedrock that stimulates innovation, safeguards inventions, and ensures a nation's technological edge in defense.

This research delves into how IP rights influence defense innovation, the creation of sophisticated military technologies, and their strategic value in the defense domain. IP rights serve as a potent catalyst for innovation within the defense sector. Patents grant inventors exclusive control over their creations for a set period, offering a window to recover investments and derive profits. This exclusivity is vital in defense, where the costs and timelines associated with research and development (R&D) are substantial. Defense technologies are not only expensive to develop but also crucial for national security, making the protection of innovative ideas through IP rights a strategic imperative (Gupta et al., 2023). The protection afforded by IP rights is essential for keeping sensitive technologies out of adversaries' hands, ensuring that groundbreaking military advancements remain confidential and proprietary. Patents allow for the strategic management of information dissemination concerning novel weapons systems, surveillance techniques, and cybersecurity measures, thereby preserving national security. In essence, the symbiosis between defense innovation and IP rights cannot be overstated. Patents and other IP forms are crucial for spurring the development of new defense technologies, securing national security interests, and bolstering the defense industrial base. As we venture further into the realms of artificial intelligence, cyber warfare, and space exploration, the strategic administration of IP rights will be paramount for nations aiming to preserve and enhance their military prowess and uphold global security.

Patents are one of the oldest forms of intellectual property protection. The patent system accelerates technological development by offering the possibility of material reward for an inventor, and at the same time, by facilitating the spread of new technological knowledge. So, It is a legal document that grants an exclusive right on the patented invention, which is a product or a process that provides, in general, a new way of doing something, or offers a new technical solution to a problem (World Intellectual Property Organization, n.d.). It is notable that patents and innovations hold a uniquely critical position in the landscape of Intellectual Property (IP) rights, especially when considering their connection to state security and defense, more so than other forms of IP like copyrights, trademarks, or trade secrets. For example, Some PCT Contracting States impose national security-based restrictions on the international application filing process, particularly when:

- ▶ The applicants are nationals of the said State;
- ▶ The applicants reside within the said State; and/or
- ▶ The invention originated within the said State. This distinct importance arises from several key aspects that directly impact a nation's security posture and defense capabilities.

Typically, an inventor is deemed authorized to submit their application to a Foreign Office if they have previously filed a corresponding application for the same invention with the relevant National Office within a specified time frame (which differs across Offices) without receiving a security directive prohibiting foreign filings, or if they have specifically sought and received approval to do so.

Therefore, if an inventor requires but has not yet obtained the necessary authorization for their international application:

- ▶ The inventor must initially file with their National Office, and
- ▶ The inventor should avoid using ePCT for drafting their international application since the draft information is stored on servers managed by the International Bureau, instead of on the inventor's personal computer or the servers belonging to the relevant National Office.

The intersection of international patent applications and national security considerations presents a critical area of legal practice and policy. Countries around the world have implemented various measures to ensure that the filing of patent applications, particularly those with potential national security implications, is carefully regulated. This paper explores these regulations, focusing on the restrictions and requirements set forth by different jurisdictions to protect national interests.

Armenia, Azerbaijan, Belgium, and Bulgaria: These countries impose restrictions based on the origin of the invention, the content of the application, and the applicant's nationality or residency, emphasizing the protection of state secrets and defense-related inventions.

China and Germany: Both countries have detailed legal frameworks focusing on inventions made within the country and applications containing state secrets, showcasing the importance of controlling the dissemination of sensitive technological information.

Denmark (Denmark, 2012): Unique in its approach, Denmark requires that certain applications related to war material are filed domestically and can be classified as "secret patents," illustrating a direct link between patent law and national defense.

Spain, Finland (Finland, 1967), France, United Kingdom, Greece, Israel, India, Italy: These jurisdictions highlight the variety of measures taken to ensure that patent applications do not compromise national security, ranging from specific restrictions on residents and nationals to considerations for defense technology.

Republic of Korea, Luxembourg, Montenegro, Malaysia, Norway (Norway, n.d.), Poland, Portugal, Romania, Russian Federation, Sweden (Sweden, n.d.), Singapore, Türkiye, United States of America, Vietnam: Each country's legal provisions underscore the global concern for securing national defense through careful management of patent applications (World Intellectual Property Organization, n.d.).

Patents and innovations, particularly in technology, cybersecurity, advanced materials, and defense systems, have a direct and tangible impact on a country's military and

defense capabilities (Jaffe & Lerner, 2004). The development of new weapons systems, surveillance technologies, communication tools, and cyber defense mechanisms can significantly enhance a nation's ability to defend itself and maintain a strategic advantage over potential adversaries. Unlike other IP rights, which primarily protect creative works or brands, patents safeguard the technical details and functionalities of these innovations, making them pivotal for state defense. The strategic value of patents in the defense sector surpasses that of other IP rights due to the sensitive nature of the technologies involved. Innovations in areas like encryption technology, drone development, and missile guidance systems are vital for national security and have implications for global stability (Morrison, 2021). The protection afforded by patents ensures that such critical technologies remain under the control of the state or authorized entities, preventing their proliferation and misuse. While copyrights and trademarks contribute to economic and cultural vitality, patents in defense and security-related innovations have a broader impact on national and global security. By fostering advancements in defense technologies, patents play a direct role in shaping the security environment, influencing deterrence strategies, and enabling states to respond to emerging threats more effectively (Tucker, 2012). This contribution is crucial in an era where technological superiority is closely linked to security and defense capabilities. The defense industry, a key component of many national economies, relies heavily on patents to protect its innovations. This protection is crucial for maintaining a competitive edge, attracting investment, and supporting research and development.

The economic health of the defense sector, safeguarded by patents, directly influences a country's ability to sustain and enhance its defense capabilities, underscoring the unique role of patents compared to other IP rights in supporting state security and defense. Patents in defense technology contribute to a state's sovereignty and independence by reducing reliance on foreign technologies and systems. Through the protection of indigenous innovations, states can develop self-reliant defense capabilities, making them less vulnerable to external pressures or supply chain disruptions. This aspect of patents is particularly significant in the context of national security, where dependence on foreign technologies can be a strategic liability (Manyika et al., n.d.). In sum, patents and innovations are more closely linked to state security and defense than other IP rights due to their direct impact on military capabilities, strategic value, contribution to national and global security, economic implications for the defense industry, and their role in ensuring sovereignty and independence. This unique position underscores the importance of fostering and protecting patents and innovations as central elements of a nation's security and defense strategy.

CONCLUSION

The relationship between intellectual property (IP) protection and global security is both complex and critical. It is essential for fostering innovation and safeguarding global

security interests. In an age where technology and knowledge are key to economic growth, but also pose security risks, establishing uniform IP protection standards is crucial. This approach helps mitigate risks related to the misuse of sensitive technologies, emphasizing the need for a unified enforcement of IP rights that aligns with global security goals. The creation of shared databases and alert systems for dual-use technologies is a proactive step towards enhancing international transparency and cooperation. These measures help ensure that technological advancements are a boon to global security rather than a threat. They allow for the early detection and control of potentially harmful technologies.

Promoting collaborative research initiatives is another strategic move. By respecting IP rights, these partnerships not only speed up scientific innovation but also incorporate safeguards against the misuse of research outcomes. This model demonstrates how IP protection can support a secure scientific progress environment, making innovation's benefits widely available yet protected from abuse. Strengthening IP enforcement capacity, especially in regions with developing IP systems, is vital for global security. International cooperation in training, resource sharing, and legal development is key to building a strong, worldwide IP enforcement framework. This ensures all countries can contribute to and benefit from a secure global innovation ecosystem. The negotiation of multilateral agreements on the control and protection of sensitive and dual-use technologies offers a way to preempt security risks. By establishing common IP protection principles, these agreements help the global community manage technological advancements without hindering scientific progress, ensuring innovations promote peace and security. In summary, IP protection and global security are deeply interconnected, requiring collaborative and nuanced strategies to ensure innovation doesn't endanger global peace and stability. Through coordinated IP standards, information sharing, joint research, capacity building, and targeted agreements, the global community can create an environment where technological advances support security, economic growth, and the well-being of all nations. This collective effort not only protects creative achievements but also ensures they serve the common good, laying the groundwork for a secure and prosperous future.

REFERENCE LIST

Denmark. (2012). *The Consolidate Secret Patents Act*. Retrieved from <https://www.wipo.int/wipolex/en/legislation/details/11456>

European Parliament and Council. (1996). Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. *Official Journal of the European Communities*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009>

Falvey, R., & Foster-McGregor, N. (2006). The Role of Intellectual Property Rights in Technology Transfer and Economic Growth: *Theory and Evidence*. Retrieved from

https://www.researchgate.net/publication/228778702_The_Role_of_Intellectual_Property_Rights_in_Technology_Transfer_and_Economic_Growth_Theory_and_Evidence

Finland. (1967). *Act on Inventions of Importance to the Defence of the Country* (551/1967). Retrieved from <https://www.wipo.int/wipolex/en/legislation/details/17891>

Gupta, K., Iancu, A., & Borges, C. (2023). *Noncompete Agreements, Innovation, and National Security*. Center for Strategic & International Studies. Retrieved from <https://www.csis.org/analysis/noncompete-agreements-innovation-and-national-security>

Jackson, A. (2024). *How Intellectual Property Law and Cybersecurity Intersect*. Retrieved from <https://www.dbllawyers.com/intellectual-property-law-cybersecurity/>

Jaffe, A. B., & Lerner, J. (2004). The Long Debate. In *Innovation and Its Discontents: How Our Broken Patent System is Endangering Innovation and Progress, and What to Do About It* (pp. 78–95). Princeton University Press. Retrieved from <http://www.jstor.org/stable/j.ctt7t655.8>

Manyika, J., McRaven, W. H., & Segal, A. (n.d.). *Innovation and National Security: Keeping Our Edge* (Independent Task Force Report No. 77). Council on Foreign Relations. Retrieved from <https://www.cfr.org/report/keeping-our-edge/>

Morrison, J. (2021). Intellectual Property & National Security. *U. Cin. Intell. Prop. & Computer L.J.*, 6(1). Retrieved from <https://scholarship.law.uc.edu/ipclj/vol6/iss1/8>

Norway. (n.d.). *Act on Inventions of Importance to the Defence of the Realm*. Retrieved from <https://www.wipo.int/wipolex/en/legislation/details/15931>

Sweden. (n.d.). *The Defense Inventions Act*. Retrieved from <https://www.wipo.int/wipolex/en/legislation/details/17716>

Tucker, J. B. (Ed.). (2012). *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies*. The MIT Press. Retrieved from <http://www.jstor.org/stable/j.ctt5vjqln>

United States Patent and Trademark Office. (n.d.). *Intellectual property and the U.S. economy*: Third edition. Retrieved from <https://www.uspto.gov/ip-policy/economic-research/intellectual-property-and-us-economy>

Wassenaar Arrangement Secretariat. (n.d.). The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Retrieved from <https://www.wassenaar.org/>

World Intellectual Property Organization. (n.d.). International applications and national security considerations. Retrieved from https://www.wipo.int/pct/en/texts/nat_sec.html

World Intellectual Property Organization. (n.d.). Technology Transfer. Retrieved from <https://www.wipo.int/technology-transfer/en/>

World Intellectual Property Organization. (n.d.). What is a patent? Retrieved from <https://www.wipo.int/patents/en/>

World Intellectual Property Organization. (n.d.). What is Intellectual Property? Retrieved from <https://www.wipo.int/about-ip/en/>

Caner Asbaş¹
Şule Erdem Tuzlukaya²

THE BRIDGE BETWEEN STRATEGIC MANAGEMENT SCHOOLS AND SECURITY STRATEGIES IN INTERNATIONAL RELATIONS: AN INTERDISCIPLINARY APPROACH

Abstract

The word "Strategos" means general in Ancient Greek while the word "Strategia", where strategy is derived from, points out the job of the general. In the field of international relations, strategy, in its narrow sense, refers to the use of military methods to achieve the aims of warfare, while designating the art of generalship similar to Ancient Greek tradition. When taken in its broad sense, the term also includes the management and directing of all resources of a nation for its political purposes. While important classical period strategists include Sun-Tzu, Thucydides and Machiavelli, in the modern period, Napoleon, Jomini, Von Clausewitz, Liddell Hart, Hobbes, Rousseau and Hegel are the leading names in this field. In this context, security in international relations is considered on the basis of maintaining existence and safety despite the internal and external threats. The concepts of strategy, which were used in almost the same sense as security until the 1980s, have since then been expanded to encompass elements such as economics, environment, population and migration, poverty, environmental problems, crime, epidemics and political relations, including the use of soft power, in addition to military issues in line with needs. In this context, security strategies can be classified under two different approaches which are realistic and liberal. In the field of business management, strategic management refers to the decisions an organization makes in order to achieve its organizational goals and their planning, implementation and evaluation, very similar to the broad definition in the field of international relations. Strategic management principles, which are frequently applied in almost every field of business management and are a part of a wide interdisciplinary relationship network, have been thoroughly studied and examined by Henry Mintzberg, a leading figure in this field. At this point, Mintzberg classified the strategies under 10 basic approaches: The Design School, The Planning School, The Positioning School, The Entrepreneurial School, The Cognitive School, The Learning School, The Power School, The Cultural School, The Environmental School and The Configuration School. In this study, by establishing connections between strategic management schools in the field of business management and organization and security strategies in the field of international relations, an effort has been made to relate the relevant literatures from

¹ Hamle RF Elektrik VE Elektronik A.Ş., canerasbas@hamlerf.com

² Atilim University, Ankara, Turkey

an interdisciplinary perspective and to build a bridge between them.

Keywords: *Henry Mintzberg, international security, strategic management, strategy schools, security strategies.*

INTRODUCTION

In Ancient Greek, the word "Strategos" is referred to as general in a military context in order to point out his capability and responsibility to develop and implement tactics in wars (Grzywaczewski, 2021). In this direction, the word "Strategia" is derived from this concept in order to express jobs of the general in a way that includes preparing war aims, generating battle plans and leading, ordering and directing the army (Oliver, 2001). In association with Ancient Greek tradition, strategy in international relations, in its narrow sense and in its first use, refers to the use of military methods to achieve the goals of warfare, the development and implementation of military tactics in this context (Ferreira, Raposo & Mainardes, 2014; Ghemawat, 2005), and the related articulation of relevant activities such as transportation and supply in line with military objectives and operations (Stead & Stead, 2008).

In the premodern and modern periods in international relations, however, with the paradigm change from the view which considers war as an event that takes place only between soldiers on the battlefield to the approach which accepts warfare as a phenomenon in which the entire nation is involved and affected, the meaning of the word strategy has also expanded and this term has begun to be used in the sense of directing and managing all the necessary and relevant resources of a nation in the relevant direction in line with its political purposes (Evered, 1983; Owens, 2007). Thus, it is possible to categorize this term in two different contents within the scope of international relations, one being operational in a narrow sense and the other being conceptual in a broad sense.

There are various important strategists in the literature who have produced significant works, developed key concepts, or enriched the concept of strategy with their field applications. For the classical period, Sun-Tzu, Thucydides and Machiavelli should be declared as the leading strategists (Hughes, 2013; Kane, 2013). Sun Tzu, known for his book *The Art of War*, which is one of the oldest works in the field of strategy, is one of the names that most deeply influenced and developed the concept of strategy with his totalistic understanding and holistic perspective on warfare (McNeilly, 2001). In addition to him, in the Greek world Thucydides presented one of the earliest examples of realist views in the field of international relations strategies with his power-based approach (Forde, 1995). As another realist strategist, Niccolo Machiavelli developed important approaches to administrative strategies with his book *Prince*, and military tactics with his book *The Art of War*; he also introduced them to the literature in connection with a comprehensive political philosophy (Gilbert, 1986).

For the modern period, Napoleon, Jomini, Von Clausewitz, Hart, Hobbes, Rousseau and Hegel can be declared the names shaping the strategy literature and understanding (de Santayana, 2020; Riley, 1982). Napoleon Bonaparte's contribution is in terms of the innovation he brought to the logic of war rather than in the theoretical field. With his goal of achieving decisive results in battle, absolute strength from the opposing side, and innovative battlefield formations, Napoleon created radical changes in the dominant military tactics of the period (van Creveld, 2011). Again, as a warrior and military tactician, Antoine-Henri Jomini brought important innovations in military practices with his emphasis on army division and speed (Alger & Paret, 1994). Carl Von Clausewitz, known for his work *On War*, stands out with his theoretical approach and philosophical investigations as well as his practical contributions (Sokolov, 2019). Liddell Hart brought a new perspective to the subject of strategy with his historical analytical approach and the cause-effect relationships he established on wars (Larson & Mearsheimer, 1991). As thinkers of the Enlightenment period, Thomas Hobbes, Jean-Jacques Rousseau and Georg Wilhelm Friedrich Hegel expanded the strategy literature with the philosophical foundations they developed on interstate relations (Riley, 1982).

The concepts of strategy, which were used in almost the same sense as security until the 1980s, have since then been expanded to encompass elements such as economics, environment, population and migration, poverty, environmental problems, crime, epidemics and political relations, including the use of soft power, in addition to military issues in line with needs (Anderson, 2014). Thus, within this concept, which has gained a wide range of uses and new approaches, security strategies, however, have continued to maintain their unique importance.

With the acceleration of interdisciplinary and multidisciplinary studies in academic fields, the concept of strategy is not limited to military service and international relations, but has gained new contexts and started to find a place in many other disciplines (Simeone, 2020). One of these is the field of business management. With the strategic management discipline in this field, the administration of organizations has begun to be carried out with long-term plans and detailed road maps, just like the management of armies and countries. Henry Mintzberg stands out as one of the prominent names in the field of strategic management, which includes the works of many important scholars (McCarthy, 2000). With his taxonomic study in the field of strategic management, Mintzberg grouped the approaches in this field under ten different schools (Mintzberg, Ahlstrand & Lampel, 1998).

In this study, it is aimed to establish an interdisciplinary bridge by connecting and relating strategic management schools in the field of business management and security strategies in the field of international relations and to ensure the permeability of information, opinions and approaches between the relevant literature. In this regard, first of all, security strategies are briefly examined, and then strategic management

schools are given with their basic characteristics. Afterwards, inferences are made by establishing an analogy between these schools and security strategies. Finally, discussion and conclusions are presented.

International Security Strategies

Ensuring domestic and international security constitutes one of the most important goals of states (Baldwin, 2018). In this direction, states develop various strategies and policies and try to protect their countries from risks and dangers by implementing them. While these strategies can target the country's direct security, they can also be expanded to include the country's commercial and industrial partners, geopolitical neighbors or other allies and advantages.

It is possible to divide security strategies into two categories: realist and liberal (Hyde-Price, 2013; Smith, 2011; Smith, 2020). The realist approach, which can be considered the modern classical view on international security strategies, focuses on states and the power relations and dominance-balance relations between these states. This approach, whose origins can be traced back to the 17th century, argues that international security is a result of the power of the state, especially its military power (Walt, 2017).

As the second approach, in liberal strategies, relations of power and superiority are replaced by interstate cooperation. Thus, interstate alliances gain importance in this approach, especially instead of increasing military capacity (Gill-Tiney, 2021). Furthermore, supranational organizations such as the European Union or specialized international organizations such as the United Nations can also be seen as an outcome of liberal security strategies (Börzel & Zürn, 2021).

As in almost every strategy study discipline, it is possible to identify generic strategies with a wide variety of different focal points for international security strategies. While some of these strategies can be directly considered within the scope of the realist approach, some of them belong to the liberal view, and some can be seen as a combination and synthesis of these two fundamental approaches. Table 1 presents some of these generic strategies.

Table 1: *Generic international security strategies*

Adaptive and Flexible Approaches	Adherence to International Law
Alliances and Partnerships	Capacity Building
Civil Society Engagement	Civil-Military Cooperation
Conflict Prevention and Resolution	Conflict Transformation
Counterterrorism	Crisis Management and Conflict Resolution
Cultural Heritage Protection	Cyber Defense and Resilience
Cybersecurity	Defense
Deterrence	Diplomacy
Disarmament	Economic Security
Educational and Cultural Exchange	Environmental Security
Gender and Security	Global Governance
Human Rights Promotion	Humanitarian Assistance and Disaster Response
Humanitarian Diplomacy	Intelligence Gathering and Analysis
Multilateralism	Non-Proliferation and Arms Control
Preventive Diplomacy	Public Diplomacy and Strategic Communication
Public-Private Partnerships	Regional Cooperation
Resilience and Preparedness	Rule of Law and Good Governance
Soft Power	Stabilization and Reconstruction
Strategic Communications	Strategic Resilience
Technology and Innovation	Transnational Crime Prevention

Strategy Safari and 10 Strategic Management Schools

Henry Mintzberg is a Canadian academician who was born in 1939. His contribution to the business management literature can be classified under two main categories as those to organization theory and those to business strategy theory. In the realm of organization theory, he developed an organizational configurations framework which identifies six types: simple structure as a characteristic type for entrepreneurship, machine bureaucracy, professional bureaucracy, diversified form, adhocracy (also called innovative organization) and missionary or idealistic organization (Mintzberg, 1980). These configurations serve as a mapping and characterization tool by covering all the different types of organizations that can survive in the organizational environment. Relatedly, Mintzberg also defined the typical mechanisms and basic parts that these organizations may have and included them in his framework.

As one of his most significant contributions, Mintzberg presented a systematical mapping and taxonomy in his book "Strategy Safari" by categorizing strategic management schools in management and organization literature into ten main classes. These schools are

The Design School, The Planning School, The Positioning School, The Entrepreneurial School, The Cognitive School, The Learning School, The Power School, The Cultural School, The Environmental School and The Configuration School (Mintzberg et al., 1998).

The Design School presents a model of strategy focusing on matching internal capabilities and external possibilities. Its origin can be dated back to the studies by Philip Selznick named *Leadership in Administration* of 1957 and Alfred D. Chandler named *Strategy and Structure* of 1962, and the concept "distinctive competence" developed by Selznick. This school advises systematic planning in strategy development starting with setting clear objectives and goals, conducting detailed and understanding analysis and continuing with implementing a structured process (Mintzberg, 1978). The framework of The Design School is based on four main principles, such as consistency, which points out the definition of consistent or at least non-contradictory policies and objectives, consonance, which is adaptivity and sensitivity of strategy to external environment, advantage, which indicates gaining and maintaining competitive advantage, and feasibility, which emphasizes the balance that should be established by strategy between available resources and problems (Mintzberg, 1994). This school, which adopts a top-down approach, considers CEO or general manager as the only strategist. Also, strategy can be implemented after it is totally formulated in a way that is unique, simple and explicit.

The Planning School, which is originated from the book *Corporate Strategy* by H. Igor Ansoff, is based on formal and comprehensive procedures, training, and analysis, and detailed data and numbers (Mintzberg, 1978). It was built on the view that strategy should be developed by planners who have special education for this task and a stand-alone planning department with direct access to top administrator (Johnson, Scholes & Whittington, 2008). This school views strategy as ordered and interdependent steps that should be followed by checklists, which is in the responsibility of the top manager.

The Positioning School, which can be considered as a combination of The Design School and The Planning School, gives a key role to strategy itself. The development of this school can be divided into three phases which are: the first wave, which is originated from mostly military strategy views such as writings of Sun Tzu who outlines the advantage of first mover and identification of limitation of generic thinking and remarks of von Clausewitz who considers strategy as finding new combinations of fundamental elements; the second wave, where special and small-scale strategies are developed for limited markets; and the third wave, where empirical search is emphasized for matching conditions and strategies, and Porter develops generic strategies (Mintzberg et al., 1998). This school, which claims that strategists select required and appropriate strategy among generic strategies instead of creating new ones, also asserts that the strategy formation process is only an effort to match performed analytical calculation to these generic strategies (Porter, 1980; Porter, 1996). Therefore, the most important and key activity is considered analysis stage.

The Entrepreneurial School focuses on the leader's intuition, judgement, wisdom, experience, insight, and views strategy formation as a visionary process (Mintzberg et al., 1998). This school is rooted in economic phenomena, especially the Schumpeterian approach to entrepreneurship (Whittington, 1993). The Entrepreneurial School, which strongly connects strategy development to the characteristics and personality of the leader claims that strategy is an outcome of the leaders' vision, perspective and mind (Kuratko, 2017; Whittington, 1993). Therefore, it is an emergent process, not a planned or configured one (Mintzberg et al., 1998). In this way, developing appropriate strategies requires experienced and somewhat charismatic leaders.

The Cognitive School, which is originated from cognitive psychology, emphasizes the importance of mind behind the strategy and is shaped around different approaches such as those that view cognition as confusion, information process, mental mapping, concept attainment, and perception construction (Mintzberg et al., 1998). In this school, strategy development is viewed as an emergent process, similarly to The Entrepreneurial School, since it is strongly related to cognitive scheme of strategist and the concepts, maps and frames in his or her mind (Acciarini, Brunetta & Boccardelli, 2021; Cyert & March, 1992). From this perspective, this school has a constructive understanding of strategy.

The Learning School, similarly to The Cognitive School, focuses on psychological operations but from the standpoint of learning, as an emergent process, whether individually or especially collectively. In this school, description is given a main role rather than prescription while strategy is considered as a combination of small-scale and short-term decisions and actions of the members of the organizations instead of a result of the total planning and efforts of the management (Argote & Miron-Spektor, 2011). In this context, due to the uncertainties and complexities in the environment, strategy development requires continuous learning from the environment and this learning process brings new and emergent strategies which are compatible with the new information gathered (Senge, 1990). Therefore, an evolutionary perspective in strategy development is adopted in this school (Tsang, 1997).

The Power School views strategy as an outcome of relationship patterns of power and politics inside the organization instead of considering it as a purely rational or cognitive process (Mintzberg, 1987). Therefore, this school puts importance on the group relations, cooperation and coalitions in terms of strategic decision making and implementation (Pfeffer, 1992). From this perspective, it has a strong relationship with political science and social psychology (Mintzberg, 1983). Furthermore, this school has a connection with game theory by defining various games in organization management, such as insurgency game, counterinsurgency game, sponsorship game, alliance-building game, empire-building game, budgeting game, expertise game, lording game, and Young Turks game (Mintzberg et al., 1998).

The Cultural School emphasizes the role of unique values, beliefs, norms, and symbols in strategy development and implementation processes by highlighting the societal and communal side of humans (Deal & Kennedy, 1982). In this context, it has the characteristics of a school in which ethnographic and anthropological perspectives predominate, that takes organization members as citizens into the account unlike previous ones (Mintzberg et al., 1998; Schein, 1985). Its main aspects can be listed as common beliefs and values, socialization and indoctrination, symbols and rituals, cultural leadership, and cultural change (Mintzberg et al., 1998).

The Environmental School is based on understanding and responding to the environment where organizations operate properly and accurately in strategical processes (Bower, 1970; Mintzberg et al., 1998). In this way, this school highlights the dynamic nature and interplay between organizations and organizational environments (Bower, 1970; Williamson, 1985). The key terms in this school can be listed as external forces, adaptation and survival, contingencies, environmental scanning, strategic response, uncertainty and complexity (Miles, & Snow, 1978; Mintzberg et al., 1998). From this perspective, a more ecological view can be traced in this school.

The Configuration School perceives the strategy development process and its operations within the framework of taking advantage of the internal characteristics of organizations (Burgelman, 1983; Mintzberg, 1978). In this regard, strategy is considered as a function and outcome of organizational structure, culture and internal harmony (Whittington, 1993). Other emphasized concepts in this theory can be listed as internal consistency, fit and congruence, contingency and strategic change (Mintzberg et al., 1998).

Text Analysis Method

In this study, a postmodernist research and analysis method supported by the German idealist school, Weber's concept of *Verstehen* and interpretative approaches has been adopted in making inferences and interpretations from strategic management schools in business management for security strategies in international relations. As the first of these concepts, the German idealist school, is a movement that started with Kant and included Fichte, another transcendental idealist, and the absolute idealists Schelling and Hegel (Ameriks, 2000). According to this movement, the features we discover in objects, in other words the information we acquire about them, are realized as a function of the image these objects create in us (Rockmore, 2010). Thus, this information becomes phenomena that we reconstruct in our minds, rather than things that objects have directly and inherently. This situation led Kant to argue that the knowledge and information production process involves the human mind as an active creator (Adams, 1997).

As another concept, interpretative approach is a philosophical movement based on the fact that thanks to human effort and ability to create meanings, the social world and the

information produced about it will and should be differentiated from producing information about the physical world and natural sciences (Saunders, Lewis & Thornhill, 2016). In this direction, contrary to the positivist approach, the researcher who conducts interpretative studies should include his own interpretation skills and outcomes as a tool in his work instead of pure objectivity, and should also make an effort to achieve results by adopting an inductive approach (Azungah, 2018; Evered & Louis, 1981; Thomas, 2006).

One of the most prominent concepts in the interpretive approach is the concept of *Verstehen*, identified with Max Weber (Tucker, 1965). In connection with the German idealist school, this epistemological concept focuses on the understanding and meaning reconstructed by people rather than on external and spontaneous reality (Salem, 2014). In this context, Dilthey associated *Verstehen* with hermeneutics and pointed out the necessity of creating internal and hidden knowledge through *Verstehen* in philosophy, religion and all kinds of critical and inferential readings, in addition to those belonging to the field of social sciences, which are shaped around the concept of verbal and non-verbal communication (Dilthey & Jameson, 1972).

The concept of postmodernism, which has been used since the 1960s as a rebellion against modernity, has become a phenomenon that is intensively studied and discussed with n Jean-François Lyotard's work titled *The Postmodern Condition* (Peters, 1995). Postmodernism replaces rational discovery through scientific research (Holtz, 2020), which was highlighted by Kuhn especially because the knowledge produced by modernist approaches has profound differences in functioning in theory and reality (Jones, 2000). Feyerabend explained this situation as modern science not applying its own formal standards and restrictions to itself (Preston, 1997).

One of the outstanding methods of the postmodernist movement is discourse analysis. Discourse analysis is a method used for the examination of any verbal or written linguistic expression or set of expressions (Kress, 1990). This method, which finds use in many fields such as sociology, anthropology, linguistics, educational sciences and cultural studies (Gee, 2014), is also used in the analysis of the relationship between discourse, power and knowledge in the field of international relations. Specifically, this analysis, which aims to discover the backgrounds of discourses and find their main meanings, can also be used to establish associations between various fields and create an intersection area.

Strategic Management Schools and Security Strategies

When generic international security strategies and strategic management schools in business management are examined comparatively, it can be noticed that the former is generally shaped around the purpose, target, method, precaution area and focused security issue, while the latter determines its focal point as concepts, strategic planning processes, the scientific field in the background of the strategic approach from which it

originates and the operational definition it adopts.

The first implication of The Design School regarding international security is to match the country's resources and opportunities with external opportunities and dangers. For example, if the country's security problems arise from border issues, the state should direct its resources to prevent this danger and try to acquire the necessary tools. Or, if the security threat is seen as a result of insufficient military training, resources should be allocated to carry out the relevant training. Another implication of this school is that the security strategy is formulated and implemented in an ordered manner, that is, in the first stage, the security target is defined; this definition is supported and operationalized by analysis, and then a structured implementation phase is carried out. In addition, with its consistency principle, this school points out the need to control and ensure the compatibility and non-conflict of the policies defined under the main security strategy, to scan the environmental compatibility of the main strategies and sub-policies with its consonance principle, and to ensure this harmony in terms of the country's resources with its feasibility principle. This school's view of the CEO as the only strategist leads us to the conclusion that in the field of international security, the only strategist is the head of state as the executor of the will of the nation. In line with this school of thought, which clearly separates the strategic planning and implementation phases, it can be argued that the planning phase should be clearly completed before the implementation of security strategies.

The Planning School attaches the importance to procedure and training points, the need for a detailed, systematic and trained bureaucracy in the field of security strategies, the need for specialized security strategy planning and analysis departments, as well as the execution of detailed and comprehensive planning and analysis activities. In this school of thought, which advises the implementation of the international security strategy plan systematically by following sequential and interdependent stages, control can be considered as the responsibility of the head of state, who is in the position of top manager. In addition, with the inference from this school, interdependent stages for security strategies should be defined and implemented decisively.

The most important inference that can be obtained for security strategies from The Positioning School, which, like the previous schools, pays special attention to analysis at the planning stage, is that this strategy indicates gaining a position according to the distance between the targeted and desired positions by choosing among generic strategies. In other words, the most appropriate generic strategy should be selected and followed to ensure security. This strategy can be determined among a wide variety of options, such as multilateralism, preventive diplomacy and military efforts. However, in order to make this choice correctly and appropriately, security threats and dangers need to be analyzed in depth, which requires the presence of specialized and competent security analysts.

The Entrepreneurial School's implications on international security strategies differ from the previous three schools due to its distinctive philosophy. The key role

that this school attributes to the leader, leadership and the characteristics of the leader can also be reflected in the head of state regarding security strategies. According to this school, a successful international security strategy emerges as a function of the wisdom, education, vision, determination and foresight of the head of state, rather than specialized and standardizable processes, and to some extent equates the head of state and the security position. In contrast to the rather deterministic security approach of the other three schools, this school emphasizes personality.

In line with The Cognitive School, which emphasizes personality like The Entrepreneurial School, but this time focuses on mental processes, international security strategies originate from the mental processes of the strategists, that is, the head of state and the administrators of the Ministry of Foreign Affairs, such as perception, interpretation and thinking. In other words, security strategists mentally reconstruct and explicate the outside world, security phenomenon and potential dangers and, as a result, create policies accordingly. This situation requires the presence of an open-minded head of state and relevant ministers and administrators who are mentally competent and have the ability to abstract in order to ensure international security.

In terms of The Learning School, since the strategy development and implementation processes bring with them learning and therefore strategic changes, instead of making long-term strategic plans that are also open to uncertainties, it can be inferred that the knowledge obtained by developing and implementing relatively short-term security strategies and even small-scale security policies should be used in the long term and this effort will automatically create the main security strategy. Another result that can be achieved from this school is that the emergent security strategy to be obtained with the adaptive and feedbacked approach will be more responsive and sensitive to environmental conditions.

When international security strategies are considered from the perspective of The Power School, it can be claimed that these strategies are the result of the inside political and administrative processes of the state and the inside power relations that emerge during these processes. Thus, the strategies that the country will follow in the international arena emerge as a result of the institutional, political and administrative interactions of the parties and sides within itself, and to some extent, internal affairs are reflected in foreign affairs. In addition, the game theory-based approaches that this school includes in its analyses can offer insightful exercises on how external security strategies are derived from internal balances.

Unlike other schools, The Cultural School gives a leading role to values and beliefs, and the results we will achieve regarding international security strategies differ greatly from them. While the rationality and mental elements dominant in other schools give way to deep-rooted cultural beliefs and practices in this school, it reveals why and how countries under similar conditions, opportunities and risks to ours develop and implement different security strategies. The effective factor at this point stands out as the state and administration

cultures of the countries. In this way, in line with the views of this school, states with different administrative understandings and traditions can have separate strategies by acting within different frameworks. In addition, with the views of this school, the international security cooperation of countries with similar nationality, language, religion, culture, ethnicity, ideology and history can be interpreted through common values.

From The Environmental School point of view, based on the ecological approach, it can be argued that the way to develop an international security strategy is to best adapt to the environment and survive thanks to this adaptation. This situation requires continuous and meticulous examination, main analysis of external forces and potential dangers, timely and appropriate strategic reactions and responses to security-related issues, and also the ability to capture the dynamism of the ecosystem in which the country is located, that is, the network of states, institutions and other actors.

In terms of The Configuration School, the most important inference that can be made for international security strategies can be made through the duality of stability versus change. According to this school of thought, which argues that strategies remain relatively constant in a configuration during stable periods, but will make a momentary jump and move to a new configuration according to changing environmental or internal conditions, and that the new stability will occur in this configuration, international security strategies also change from one state to another according to changing environmental conditions and should "leap" instantaneously. This school of thought is especially important due to the radical change it offers and the opportunity to take a new position in the face of unexpected but potentially high-risk and suddenly developing issues. For example, an unforeseen danger of war, terrorist attack or high tension between states will require such a leap in security strategy, and as long as the danger persists, a relatively stable course will be followed in the newly reached configuration.

CONCLUSION

In conclusion, this study brings a new perspective to security strategies in the field of international relations with the inferences obtained from strategic management schools in the field of business management, and also makes various comments about security strategies through the frameworks provided by strategic management schools. In the study, ten strategic management schools identified by Mintzberg are explained with their basic principles and approaches, and then the possible consequences of these schools on security strategies are discussed.

As a result of the comparative evaluation, it has been seen that it is possible to apply strategic management schools separately to security strategies, as well as combining two or more of them and integrating them into security strategy development and implementation efforts. Since these schools offer conceptual and academic disci-

plinary views, their operationalization can be performed in various ways. Moreover, these schools can also serve as philosophical foundations and application frameworks for approaches within the realist and liberal view. As an approach that has not been studied much, this interdisciplinary relationship may open the door to many new studies.

REFERENCE LIST

- Acciarini, C., Brunetta, F., & Boccardelli, P. (2021). Cognitive biases and decision-making strategies in times of change: A systematic literature review. *Management Decision*, 59(3), 638-652. <https://doi.org/10.1108/MD-07-2019-1006>
- Adams, R. M. (1997). Things in themselves. *Philosophy and Phenomenological Research*, 57(4), 801-825. <https://doi.org/10.2307/2953804>
- Alger, J. I., & Paret, P. (1994). *Antoine-Henri Jomini: A Bibliographical Survey*. West Point, NY: National Defense University.
- Ameriks, K. (2000). Introduction: Interpreting German idealism. In K. Ameriks (Ed.), *The Cambridge Companion to German Idealism* (pp. 1-17). Cambridge, England: Cambridge University Press.
- Anderson, J. C. (2014). *Changing the Game: Human Security as Grand Strategy*. Carlisle, PA: Peacekeeping and Stability Operations Institute, U.S. Army War College.
- Argote, L., & Miron-Spektor, E. (2011). *Organizational learning: From experience to knowledge*. *Organization Science*, 22(5), 1123-1137. <https://doi.org/10.1287/orsc.1100.0621>
- Azungah, T. (2018). Qualitative research: Deductive and inductive approaches to data analysis. *Qualitative Research Journal*, 18(4), 383-400.
- Baldwin, D. A. (2018). The concept of security. In M. Sheehan (Ed.), *National and International Security* (pp. 41-64). London, England: Routledge.
- Bower, J. L. (1970). *Managing the Resource Allocation Process: A Study of Corporate Planning and Investment*. Boston, MA: Harvard Business School Press.
- Börzel, T. A., & Zürn, M. (2021). Contestations of the Liberal International Order: From liberal multilateralism to postnational liberalism. *International Organization*, 75(2), 282-305. <https://doi.org/10.1017/s0020818320000570>
- Burgelman, R. A. (1983). A process model of internal corporate venturing in the diversified major firm. *Administrative Science Quarterly*, 28(2), 223-244. <https://doi.org/10.2307/2392619>
- Cyert, R. M., & March, J. G. (1992). *A Behavioral Theory of the Firm* (2nd ed). Hoboken, NJ: Blackwell Publishers.
- David, F. R., & David, F. R. (2017). *Strategic Management: Concepts and Cases* (16th ed). London, England: Pearson.

de Santayana, J. P. (2020). The interpreters of Napoleon: Total war and decisive battle. *Araucaria-Revista Iberoamericana de Filosofía Política y Humanidades*, 22(44), 387-398. <https://doi.org/10.12795/araucaria.2020.i44.18>

Deal, T. E., & Kennedy, A. A. (1982). *Corporate Cultures: The Rites and Rituals of Corporate Life*. Reading, MA: Addison-Wesley.

Dilthey, W., & Jameson, F. (1972). The rise of hermeneutics. *New Literary History*, 3(2), 229-244. <https://doi.org/10.2307/468313>

Evered, R. (1983). So what is strategy? *Long Range Planning*, 16(3), 57-72. [https://doi.org/10.1016/0024-6301\(83\)90032-8](https://doi.org/10.1016/0024-6301(83)90032-8)

Evered, R., & Louis, M. R. (1981). Alternative perspectives in the organisational sciences: 'inquiry from the inside' and 'inquiry from the outside'. *Academy of Management Review*, 6(3), 385-395. <https://doi.org/10.2307/257374>

Ferreira, J. J., Raposo, M. L., & Mainardes, E. W. (2014). Strategy and strategic management concepts: Are they recognized by management students? *E+M Ekonomie a Management*, 17(1), 43-61. <https://doi.org/10.15240/tul/004/2014-1-004>

Forde, S. (1995). International realism and the science of politics: Thucydides, Machiavelli, and neorealism. *International Studies Quarterly*, 39(2), 141-160. <https://doi.org/10.2307/2600844>

Gee, J. P. (2014). *An Introduction to Discourse Analysis: Theory and Method*. London, England: Routledge.

Gilbert, F. (1986). Machiavelli: The Renaissance of the Art of War. In P. Paret, G. A. Craig, & F. Gilbert (Eds.), *Makers of Modern Strategy from Machiavelli to the Nuclear Age* (pp. 11-31). Princeton, NJ: Princeton University Press.

Grzywaczewski, J. (2021). Saint Mary as a hetman based on the Akathist Hymn. *Vox Patronum*, 80, 221-238. <https://doi.org/10.31743/vp.12275>

Herberg-Rothe, A. (2014). Clausewitz's concept of strategy – Balancing purpose, aims and means. *Journal of Strategic Studies*, 36(7), 903-925. <https://doi.org/10.1080/01402390.2013.853175>

Ghemawat, P. (2005). *Strategy and the Business Landscape: Core Concepts* (2nd ed). Hoboken, NJ: Prentice-Hall.

Gill-Tiney, P. (2021). A liberal peace? The growth of liberal norms and the decline of interstate violence. *Journal of Conflict Resolution*, 66(3), 413-442. <https://doi.org/10.1177/002200272111035554>

Holtz, P. (2020). Does postmodernism really entail a disregard for the truth? Similarities and differences in postmodern and critical rationalist conceptualizations of truth, progress, and empirical research methods. *Frontiers in Psychology*, 11, <https://doi.org/10.3389/fpsyg.2020.545959>

Hughes, R. G. (2013). Strategists and intelligence. In R. Dover, M. Goodman, & C. Hillebrand (Eds.), *Routledge Companion to Intelligence Studies* (pp. 50-58). London, England: Routledge.

Hyde-Price, A. (2013). Neither realism nor liberalism: New Directions in theorizing EU security policy. *Contemporary Security Policy*, 34(2), 397-408. <https://doi.org/10.1080/13523260.2013.808070>

Johnson, G., Scholes, K., & Whittington, R. (2008). *Exploring Corporate Strategy: Text and Cases* (8th Edition). Hoboken, NJ: Prentice Hall.

Jones, C. A. (2000). The modernist paradigm: The artworld and Thomas Kuhn. *Critical Inquiry*, 26(3), 488-528. <https://doi.org/10.1086/448976>

Kane, T. M. (2013). *Strategy: Key Thinkers*. Cambridge, England: Polity Press.

Kress, G. (1990). Critical discourse analysis. *Annual Review of Applied Linguistics*, 11, 84-99. <https://doi.org/10.1017/S0267190500001975>

Kuratko, D. F. (2017). *Entrepreneurship: Theory, Process, Practice* (10th ed). Boston, MA: Cengage Learning.

Larson, R. H., & Mearsheimer, J. J. (1991). Liddell Hart and the Weight of History. *The American Historical Review*, 96(1), 171-172. <https://doi.org/10.2307/2164088>

McCarthy, D. J. (2000). View from the top: Henry Mintzberg on strategy and management. *Academy of Management Perspectives*, 14(3), 31-39. <https://doi.org/10.5465/ame.2000.4468063>

McNeilly, M. (2001). *Sun Tzu and the Art of Modern Warfare*. Oxford, England: Oxford University Press.

Miles, R. E., & Snow, C. C. (1978). *Organizational Strategy, Structure, and Process*. New York, NY: McGraw-Hill.

Mintzberg, H. (1978). Patterns in strategy formation. *Management Science*, 24(9), 934-948. <https://doi.org/10.1287/mnsc.24.9.934>

Mintzberg, H. (1980). Structure in 5's: A Synthesis of the Research on Organization Design. *Management Science*, 26(3), 322-341.

Mintzberg, H. (1983). *Power in and around Organizations*. Hoboken, NJ: Prentice-Hall.

Mintzberg, H. (1987). Crafting strategy. *Harvard Business Review*, 65, 66-75.

Mintzberg, H. (1994). *The Rise and Fall of Strategic Planning: Reconceiving Roles of Planning, Plans, Planners*. Los Angeles, CA: The Free Press.

Mintzberg, H., Ahlstrand, B., & Lampel, J. (1998). *Strategy Safari: A Guided Tour through the Wilds of Strategic Management*. Los Angeles, CA: The Free Press.

Oliver, R. W. (2001). Real-time strategy: What is strategy, anyway? *Journal of Business Strategy*, 22(6), 7-10. <https://doi.org/10.1108/eb040202>

Owens, M. T. (2007). Strategy and the strategic way of thinking. *Naval War College Review*, 60(4), 111-124.

- Peters, M. (1995). Education and the Postmodern Condition: REVISITING Jean-Francois Lyotard. *Journal of Philosophy of Education*, 29(3), 387-400. <https://doi.org/10.1111/j.1467-9752.1995.tb00367.x>
- Pfeffer, J. (1992). *Managing with Power: Politics and Influence in Organizations*. Harvard, MA: Harvard Business Press.
- Porter, M. E. (1980). *Competitive Strategy: Techniques for Analyzing Industries and Competitors*. Los Angeles, CA: The Free Press.
- Porter, M. E. (1996). What is strategy? *Harvard Business Review*, 74, 61-78.
- Preston, J. (1997). *Feyerabend: Philosophy, Science and Society*. Cambridge, England: Polity Press.
- Riley, P. (1982). *Will and Political Legitimacy: A Critical Exposition of Social Contract Theory in Hobbes, Locke, Rousseau, Kant, and Hegel*. Harvard, MA: Harvard University Press.
- Rockmore, T. (2010). Fichte, German idealism and the thing in itself. In D. Breazeale, & T. Rockmore (Eds.), *Fichte, German Idealism, and Early Romanticism* (pp. 9-20). Amsterdam, The Netherlands: Rodopi.
- Salem, P. E. of. (2014). *Early Theorists and the Science of Society*. Pasadena, California: Salem Press.
- Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students* (7th Edition). Harlow, England: Pearson.
- Schein, E. H. (1985). *Organizational Culture and Leadership*. Hoboken, NJ: Jossey-Bass.
- Senge, P. M. (1990). *The Fifth Discipline: The Art and Practice of the Learning Organization*. New York, NY: Doubleday/Currency.
- Simeone, L. (2020). Characterizing strategic design processes in relation to definitions of strategy from military, business and management Studies. *The Design Journal*, 23(4), 515-534. <https://doi.org/10.1080/14606925.2020.1758472>
- Smith, M. E. (2011). A liberal grand strategy in a realist world? power, purpose and the EU's Changing Global Role. *Journal of European Public Policy*, 18(2), 144-163. <https://doi.org/10.1080/13501763.2011.544487>
- Smith, E. (2020). The traditional routes to security: Realism and liberalism. In P. Hough, B. Pilbeam, & W. Stokes (Eds.), *International Security Studies: Theory and Practice* (pp. 12-29). London, England: Routledge.
- Sokolov, E. (2019). Modernity of war: Carl von Clausewitz and his theory. *Philosophical Literary Journal Logos*, 29(3), 67-98. <https://doi.org/10.22394/0869-5377-2019-3-67-94>
- Stead, J. G., & Stead, W. E. (2008). Sustainable strategic management: An evolutionary perspective. *International Journal of Sustainable Strategic Management*, 1(1), 62-81. <https://doi.org/10.1504/ijssm.2008.018127>

Thomas, D. R. (2006). A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation*, 27(2), 237-246. <https://doi.org/10.1177/1098214005283748>

Tsang, E. W. K. (1997). Organizational learning and the learning organization: A dichotomy between descriptive and prescriptive research. *Human Relations*, 50(1), 73-89. <https://doi.org/10.1177/001872679705000104>

Tucker, W. T. (1965). Max Weber's Verstehen. *The Sociological Quarterly*, 6(2), 1157-165. <https://doi.org/10.1111/j.1533-8525.1965.tb01649.x>

van Creveld, M. (2011). Napoleon and the dawn of operational warfare. In J. A. Olsen, & M. van Creveld (Eds.), *The Evolution of Operational Art from Napoleon to the Present* (pp. 9-34). Oxford, England: Oxford University Press.

Walt, S. M. (2017). *Realism and security*. *Oxford Research Encyclopedia of International Studies*. Oxford, England: Oxford University Press. <https://doi.org/10.1093/acrefore/9780190846626.013.286>

Whittington, R. (1993). *What is Strategy and Does It Matter?*. London, England: Routledge.

Williamson, O. E. (1985). *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting*. Los Angeles, CA: The Free Press.

*Srdjan Zgonjanin*¹

*Zoran Obradović*²

RESERVE MILITARY FORCES OF NEUTRAL COUNTRIES AT MODERN CONFLICTS

Abstract

The current operational environment is increasingly complex, dynamic and unpredictable. Military operations vary in duration and intensity, but regardless of the type, they represent a major challenge for the conflicting parties due to the complexity of the identified threats and the multitude of actors present in the area of operation. The latest conflicts in Ukraine, and before that in Syria, Iraq, Afghanistan, and even the former SFRY, show that well-sized, trained and equipped reserve military forces are necessary in the defense of the national interests and the achievement of the military and political goals of the state. The question arises: what is the role of reserve forces of militarily neutral countries in modern armed conflicts? An analysis of the organization, size, and composition of reserve forces of states that have opted for a militarily neutral status in international relations, as well as the concept of total defense, will lead us to the conclusion that our security forces must also have a strong reserve component that will be capable of supporting constantly engaged groups in future conflicts of a changed physiognomy.

Keywords: *reserve composition, modern conflict, neutrality, total defense.*

The organization of the armed forces of neighboring states, states that have opted for a militarily "neutral status" in international relations, and ultimately the armed forces of great powers is determined by: the types and nature of security challenges and threats; the defense interests of states; the necessary operational capabilities; the available defense resources and the degree of integration of the country into international security processes. The armed forces of all states are staffed in a similar way, mostly by a professional army, less and less by general military conscription, but almost all states count on a strong and capable reserve force. It is also evident that the physiognomy of modern conflicts has changed, especially in the last 30 years. The organization and size of the reserve force differs from state to state.

The concept of reserve forces dates back to ancient times when soldiers were required to serve in the military during wartime, but were allowed to return to their civilian lives in peacetime. In modern times, reserve forces have become an integral

¹ School of National Defense, University of Defense in Belgrade, Serbia, srdjanzgonjanin007@gmail.com

² School of National Defense, University of Defense in Belgrade, Serbia

part of many military organizations around the world. The size and composition of reserve forces varies greatly depending on the country and the specific military organization. Today, reserve forces can be simply defined as units - commands, permanent or temporary structures that are mainly filled with personnel deployed in reserve. What is undeniable is that it is of crucial importance for all armies to have the necessary reserve forces, as well as material reserves, which cannot be acquired in a short period of time and to have supplies of materials and services provided by industry. The army must have the ability to use the knowledge (military and civilian), skills and abilities possessed by reserve personnel, to make timely selection and quickly fill missing specialties, the ability to quickly integrate into the war structure, using selective recruitment and mobilization, all with the aim of developing the ability to perform operational tasks.

Considering the physiognomy of conflicts in the recent past, including conflicts that have occurred in our region, we realize that the reserve composition of the conflicting parties was one of the most important factors in their course and outcome.

In considering proposals for the dimensioning and development of the capabilities of our reserve military forces, significant experience is provided by studying, analyzing and comparing the size and composition of our state's reserve forces with reserve forces in the armed forces in the world, and primarily with states that have opted for a militarily neutral status in international relations as well as for the concept of total defense, and in the conditions of the modern global and regional environment, as well as the physiognomy of modern conflicts in the world.

What are the characteristics of modern conflicts and what parameters that influence the very "design" of armed forces could be recognized and distinguished in them?

Armed conflict is a phenomenon that is constantly developing, changing, adapting and requires a flexible and adaptable approach to military operations. Because "war as a battle on the battlefield between manpower and machinery, war as a massive decisive event in an international dispute, such a war no longer exists" (Smith, 2007: 13). German General Franz Uhle-Nettler wrote: "Previously, the commander could be sure that the future war would be partially similar to past and current wars. This allowed him to analyze the appropriate tactics from the past and the present. The one who commands the army today no longer has this opportunity. He only knows that who fails to adopt the experiences of the past war will certainly lose the next one" (Williams et al., 1989: 22-26).

Adopting experiences for contemporary conflicts means knowing the wars of the past and their physiognomy. The wars of the first generation (Napoleonic Wars) were characterized by mass armies, while the wars of the second generation (World War I) were characterized by the participation of mass armies, but firepower emerged as the dominant element. The war of the third generation (World War II) is characterized by blitzkrieg, i.e. the rapid transition from one maneuver to the next. The war of the fourth generation (Vietnam, Iraq) is characterized by the "isolation of the battlefield", i.e. the

"separation" of the main defense forces from the reinforcement and support forces, by fire strikes from land, sea and air, and the destruction of the armed forces by elements.

Fourth-generation wars are characterized by disorientation of the enemy. According to William S. Lind, modern war has already entered the fifth-generation war in most respects (NATO aggression against the FRY, the armed conflict in Syria, Russia's Special Military Operation in Ukraine) and is characterized by a crisis of state legitimacy, i.e. the loss of the state monopoly over war, primarily the loss of loyalty of its citizens, the rise of non-state entities whose loyalty is managed by organizations-states-individuals who wage wars. These entities can be armed criminal, religious, racial and ethnic groups within races, tribes, business enterprises and ideologies. Their diversity is almost unlimited (Williams et al., 1989: 6).

In the last two decades, 95% of armed conflicts have occurred within states, not between them (Sretenović, 2011: 291). Modern armed conflicts are characterized by completely non-linear methods of combat that disorient the enemy and aim at his mental and moral-psychological paralysis, and their goal is to cause the collapse of the enemy from within, and not to physically destroy his armed forces. The combat space of fourth-generation wars does not only include the operational space of the armed forces, but also encompasses more or less the entire society of the enemy. In modern asymmetric conflicts, the goals of the participants are not limited to military goals, but include political, social, economic, and even psychological aspects. Modern conflicts are a logical choice for terrorist groups and other asymmetric participants. The changing nature of modern war has created new characteristics: special warfare, asymmetric and non-linear character, the influence of the media, etc. The battlefield in modern conflicts is unstable, without firm borders, and permeates civilian life and every pore of society.

Global trends in the changing modern environment will affect the sources, causes and methods of conflict resolution. The application of artificial intelligence, robots, adversarial and non-contact warfare and the massive implementation of actions in the information and cyber dimensions will require the development of new, or rather, the improvement of existing concepts of warfare (Ministry of Defence, 2021). It is a historical fact that technological progress causes a revolution in military affairs, and not vice versa.

Modern operations take place in conditions of "chaos", i.e. in a nonlinear sphere and asymmetry. They are characterized by frequent changes in the situation, which create a variety of problems that need to be urgently resolved. A wide range of different influences indicates the need for permanent reflection and a significant exchange of experiences in this field between scientists and experts from military and civilian structures within the state, but also within the entire international community.

Considering the above parameters, we can conclude that the basic characteristics of modern armed conflicts are (Docslib):

- unpredictability of occurrence;
- the presence of a wide range of military, political, economic and other goals;

- integrated use of military forces and forces and assets that do not have a primary military purpose;
- shortening the response time;
- improvement of the command system and the transition from a linear command system to a network system;
- the increasing role of modern highly efficient combat systems (the use of high-precision weapons of great destructive power, remotely controlled combat systems and systems for conducting electronic and cyber operations);
- simultaneous use of forces in all parts of the geographical space (land, water, air, space) and the possibility of exerting action from them;
- the importance of media and information on the course and outcome of an armed conflict;
- the significant role of information and psychological action.

The question arises: where is the place and what is the role of reserve military forces, especially those of neutral countries, in this operational environment with its changed character and completely new features of modern armed conflicts?

Reserve forces have a long history, and the concept of the citizen-soldier dates back to ancient Greece. However, modern reserve forces are organized differently and have different roles and functions. Today's reserve forces are an integral part of the military and can be used in a variety of ways, primarily in homeland defense, in support of regular forces, and can be used in peacekeeping missions. This is because the changing nature of modern conflicts has changed the concept of using reserve forces.

Reserve forces make up more than half of the fighting strength of NATO member countries' armies. In fact, the organization, composition, mission, and training levels of reserve forces vary greatly across the Alliance. But what reserve forces have in common is that they play an important role across the spectrum of national and NATO defense structures and in the event of a crisis, they are and will be required to perform tasks alongside regular forces. Reserve forces are no longer considered a force of last resort, but are now recognized as an indispensable factor in the armed forces (NRFC).

How reserve forces have been and are being used in modern conflicts can be illustrated by the experiences of military operations in the Arab-Israeli wars, in Iraq, Afghanistan, Syria, Vietnam, and Ukraine.

The use of reserve forces in the military operations of the United States of America (USA), as a global military power, in Afghanistan, Iraq, and Syria was crucial to the success of these campaigns. Reserve forces provided the active military with the necessary operational capabilities and strategic depth to expand its collective capabilities. The US Army as a whole has reached a balance of 48 percent regular and 52 percent reserve components, a level reached in fiscal 2015 and projected to continue until at least 2025 (NRFC). This is currently the largest operational command staffed with reserve

personnel. This type of reserve formation was used in all US Army operations.

In Afghanistan, the reserve component has been used intensively since the beginning of operations in the "Enduring Freedom" campaign in 2001. Reserve soldiers are deployed in a variety of roles, including combat and logistical support, as well as intelligence. According to the official website, Army Reserves from September 2021, over 35,000 reserve soldiers have been mobilized in Afghanistan since 2001 (Perry et al., 2015). They have provided key support to US forces in conducting operations (clearing road communications, providing medical support, and conducting intelligence operations). Reserve military forces have provided the necessary level of professional competence in areas such as civil-military cooperation, which has been crucial for building relationships with local communities and promoting stability in Afghanistan.

In Iraq, the Army Reserve played a vital role in Operations Iraqi Freedom and Inherent Resolve. In these operations, the Army Reserve was deployed in various units, but they mainly performed tasks in combat and logistical support units, as well as Military Police units. According to the aforementioned Army Reserve website from September 2021, these units provided support to US forces in providing convoy security, medical support, and detainee security and escort. The Army Reserve also played a key role in training Iraqi security forces, which was essential for promoting stability and security.

In Syria, the Reserve was deployed in support of Operation Inherent Resolve (Perry et al., 2015). Reservists are deployed in a variety of roles, including intelligence, logistics, and military police. Over 8,000 reservists have been mobilized in Syria.

As we can see, the reserve component of the army played a vital role in US operations in Afghanistan, Iraq and Syria. Reserve military forces have provided critical support to the US armed forces in various roles, in combat operations, logistical support operations and intelligence operations.

Throughout history, there have been many examples where reserve forces have played a significant role in the defense of small countries from aggressive acts of great powers by using military experiences of partisan and guerrilla warfare. Examples include partisan units in our region during World War II, the Vietnam War and the resistance of the Afghan people first to the USSR and in the recent past to the USA. This is still one of the models in modern conflicts, where small countries can provide successful resistance to a much superior enemy. An obvious example is the war in Ukraine, where the Ukrainian leadership mobilized the entire possible reserve force over the past eight years of conflict with the Russian armed forces. After mobilization, the reserve force was trained and then successively involved in combat operations, first in the Donbas region and then on the territory of the entire Ukraine. Ukrainian reserve military forces were integrated with operational forces and were often used at the center of defense, for the defense of populated areas, defense of isolated directions and fortified areas where individual units of the reserve forces (territorial defense) demonstrated very high operational

capability (110th TD Brigade in the Vuhledar region, 112th in the Avdeyevka region). With the support of regular units of the reserve military forces (TD of Ukraine), they carried out very successful offensive operations (in the Kharkiv and Zaporizhia regions).

The Israel Defense Forces (IDF) also rely heavily on their army reserves (Levinson, 2022). These reservists are citizens who have served their mandatory military service (women 2 years, men 3 years), and are then called up to serve periodically throughout their lives. The Israeli authorities estimate that, if necessary, Israel can mobilize its entire military potential within 48 hours and deploy it as a highly trained and equipped military force.

The Socialist Federal Republic of Yugoslavia (SFRY) was, along with Switzerland, Finland, Sweden, Austria and Singapore, one of the neutral states that implemented the concept of total defense in its defense system. The essence of this concept was defense against external threats by relying on its own forces. It was based on a combination of the capabilities of the armed forces with developed civil defense and an attempt to connect the economic and political infrastructure in defense planning. The concept was based on the creation of the armed forces on the basis of an "armed people". The most important characteristics of the concept were its deterrent function in peace, in a state of emergency and in war, as well as reliance on its own capacities in war (Strategija ONO i DSZ, 1987). In the modern operational environment, due to the transnational nature of threats, the above-mentioned states found themselves faced with the challenge of redefining the concept of "total defense", and the need arose to, in addition to relying on their own forces, possibly engage in partnerships and alliances. This concept was primarily based on self-sufficiency in every vector, and especially economic sovereignty and the determination to allocate the necessary part of the economic potential for defense itself.

Table 1 presents a comparative analysis of states that have been implementing the concept of total defense for many years through four important parameters of power that characterize a sovereign state, namely: the area of the territory expressed in km², the number of inhabitants, the number of soldiers, and the percentage of GDP allocated to the military budget.

Table 1. Comparative analysis of the power of states with the concept of total defense

	Area of the territory	Population (millions)	Number of soldiers (active/reserve)	Military budget
Finland	(km ²)	5.503.000	22.200/350.000	1,23% GDP
Serbia	88.631	6.982.604	30.000/440.000	1,40% GDP
Austria	83.879	8.773.000	57.133/350.000	0,7 % GDP
Denmark	42.933	5.749.000	12.500/75.000	1,12% GDP
Switzerland	41.285	8.420.000	21.000/242.000	0,9 % GDP
Singapore	693	5.612.000	72.500/900.000	4,9 % GDP

Source: Jokić, Ž. (2020). *Problem primene koncepta totalne odbrane u Republici Srbiji*, Univerzitet odbrane, Beograd.

From this table it can be seen that in terms of the area of the territory, if we exclude Finland with an extremely large area and Singapore with an extremely small area, the Republic of Serbia has a larger territory than other countries. In terms of human potential, both total and military capable, Serbia is on average with the above countries. In terms of the military budget, the amount of \$ 726 million or 1.40% of GDP in 2018, according to sources from the Ministry of Defense, is certainly below the 2% of GDP recommended by NATO. In percentage terms, the Republic of Serbia is even above the average in relation to the above countries, with the exception of Singapore, but the percentage does not mean the total amount. Moreover, unlike other neutral European countries, Serbia is relatively economically underdeveloped, which further affects the total GDP, and thus the allocation for the military. In order to carry out a complete analysis of the financial resources allocated to the military in the above-mentioned countries, it is necessary to know the budgets of these countries, which requires a deeper analysis.

The commitment to a policy of military neutrality has significant repercussions on defense policy, as indicated by the practice and experience of militarily neutral countries. Namely, today absolutely all European countries that build their strategic commitment on the basis of military neutrality, such as Switzerland, Austria and Ireland, base their defense policy on the concept of total defense. Militarily neutral countries are forced to develop defense strategies and doctrines based on their own national defense capacities. The defense policies of absolutely all militarily neutral states are based on the concept of total defense, which implies the integral engagement of all defense entities and defense potentials, both military and civilian, in order to strengthen the defense capabilities of the state. Militarily neutral states certainly have different approaches to security and defense issues, in accordance with different traditions, geopolitical position, national interests, etc. However, what they have in common are strong defense capabilities of the state, which are achieved through the development and implementation of the concept of total defense. This includes strong armed forces, as a reliable factor of deterrence against armed aggression, then a developed recruitment system for replenishing the armed forces, a numerically respectable and trained reserve force, a developed civil defense system, which aims to protect the population during crises, a strong defense industry that should, to the greatest extent possible, meet the needs of the armed forces, etc.

In the concept of total defense, the armed forces have an important place, but they are by no means alone in defense affairs. On the contrary, the fact that defense is total means that it concerns the entire society, and not only those who of their own free will (voluntarily) choose the military profession as their life profession and join the professional or active army. However, the place of the army remains special, because it represents a deterrent factor and is the only one with a developed ability to wage armed struggle. Therefore, the question of the composition, size and equipment of the army,

determined by numerous factors ³, is of great importance even in neutral countries.

The concept of total defense places its hopes in a relatively large number of relatively well-trained soldiers. The question arises as to how to ensure a sufficient number of such soldiers and how to motivate citizens for active participation in potential military tasks, civil protection tasks and other tasks that give credibility to the defense capabilities of a neutral state? It is quite certain that compulsory military service ensures that a relatively large number of people are trained to perform various military tasks, which, in turn, contributes to the efficiency of the army in the event of the need to mobilize and replenish the army to its war formation. In short, it ensures the sufficiency of reserve military forces.

For a neutral state, which has opted for the concept of total defense, as the only possible concept for developing respectable defense capabilities, a small professional army is not enough. Developed and trained reserve military forces are needed to participate in both military and civil defense tasks, because civil defense, in addition to non-military ones, must also respond to military challenges, risks and threats to their security. In military defense tasks, in addition to the peacetime composition, the reserve military forces are the first and main bearer of all tasks. In civil defense tasks, as a supporting element, they are certainly extremely important. Therefore, reserve military forces must develop capabilities in order to respond to the tasks and requirements of the total defense concept, both in military and civil defense.

Most countries that have adopted the concept of total national defense, in which the wartime army is larger than the peacetime army, rely on compulsory military service to ensure the replenishment of the reserve contingent as a primary goal and, as a secondary and no less important, the replenishment of the reserve contingent with qualified personnel. Sweden abolished compulsory military service in 2010, but in 2018 it was reinstated due to new security dynamics in the region. Similarly, Lithuania abolished compulsory military service in 2008, but in 2015 it was reinstated due to the newly emerging geopolitical situation and the shortage of personnel in the armed forces. Norway has developed a hybrid model of compulsory military service, which since 2016 includes women. Everyone is required to register, while between 15 and 20% of the most motivated and able citizens serve their military service on an annual basis. In Singapore, all men over the age of 18 are required to complete two years of national service in the armed forces, civil defense forces, or police. The only country that has adopted the concept of total defense without mandatory military service is Latvia, which abolished it in early 2007. Instead, Latvia has chosen to develop a professional army and a National Guard - a territorial defense force, which is recruited on a voluntary basis.

³ "The composition, size and equipment of the armed forces are determined, first of all, by the political system of the country, the level of overall development, the geostrategic position of the country, demographic possibilities, military and defense doctrine." Srđan Blagojević, Ivan Gvozdenović, Slobodan Anđelković, "The Importance of Harmonizing Political and Defense Goals for the Security of the State and Society", cited work, p. 139.

States that have adopted the concept of total defense usually have some form of territorial defense force, and thus the defense of the state is organized through special units, most often volunteer homeland or national guards composed of professional soldiers or conscripts with basic military and civilian training, with the responsibility to protect and monitor the territory of the state and to assist the entire society in the event of a crisis. In Sweden (while it was militarily neutral), these units operated during forest fires, floods, pandemics, and searches for missing people, and in the event of a military attack they would be the first to enter the field until the regular military forces mobilized and prepared for action. In Latvia, the territorial defense forces are trained for anti-tank and anti-aircraft operations, carrying out activities related to the suppression of weapons of mass destruction, as well as engineering tasks. The Lithuanian Territorial Defence Forces participate in urban warfare, participate in anti-tank operations, and may also participate in international operations. In peacetime, these units are most often trained by reservists and respond to crisis situations, assist in rescue missions, and cooperate with the police, border police, and firefighting units. From the experiences of these countries, we see that reserve military forces have their own inherent role in military defense, but they certainly have their own role in civil defense within the concept of total defense.

From the examples above, we can see that one of the primary benefits of reserve forces is their ability to supplement the regular military in times of crisis or war. These forces can provide additional forces to support active military units, ensuring the smooth running of operations. This can be especially important in protracted conflicts, where regular military units may be stretched and insufficiently capable of sustaining the intensity of operations. By supplementing these units, the reserve component helps to alleviate the burden on regular military units, ensuring that they remain efficient and effective. While there are challenges associated with the use of reserve forces, careful planning and coordination can help overcome these challenges and ensure that reserve forces are an effective and valuable asset to modern military operations.

Reserve forces therefore play a significant role in modern security threats, including in modern warfare. These forces, composed of trained citizens who are not currently serving in the active military, are often called upon to supplement the regular military during a crisis or war. This includes soldiers, sailors, airmen, and marines who have completed basic military training and can be quickly mobilized to support regular units. Reserve forces can also be called upon to provide additional support to law enforcement agencies and first responders during crises or natural disasters. This includes search and rescue operations, maintaining public order, and providing medical assistance. Therefore, reserve forces are also used in the modern era as a response to non-military challenges, risks, and threats to the security of states.

Despite these advantages, there are also certain challenges associated with the use of reserve forces in the world. One of the primary challenges is maintaining the readiness

of these units. Reserve forces are typically comprised of individuals who perform civilian jobs and responsibilities outside of the military. This can make it difficult to ensure that they are adequately trained and ready to serve when called upon. In addition, there can be communication and coordination problems between regular and reserve units, especially in joint operations, operations with other countries or organizations where different units may have different procedures and protocols. This challenge can be addressed through improved communication and coordination between regular and reserve units, as well as through joint training and exercises that help build trust and rapport between them.

To address these challenges, it is important to ensure that reserve forces are regularly trained and effectively integrated into military operations. This includes providing opportunities for ongoing training and ensuring that reservists have access to the necessary resources and equipment to effectively perform their duties.

In the future, the use of reserve forces is likely to become even more important in ensuring the success of military operations. As the nature of warfare continues to evolve, the military will need to be more flexible and adaptable in its approach. Reserve forces must provide the necessary flexibility and adaptability to respond to changing situations and support the regular military in its operations.

Looking ahead, there are several potential directions for the gradual transformation and use of reserve forces in national defense and security. Reserve military forces within the armed forces around the world, together with active forces, are developing capabilities to use and counter transnational terrorism and organized crime, cyber and hybrid threats, ethnic and religious extremism, migration, proliferation of weapons of mass destruction, environmental degradation, and the spread of infectious diseases in humans and animals. Climate change and the increasing scarcity of energy and other natural resources can also be a cause of confrontation and conflicts. The use of the reserve component requires the development of capabilities in response to these threats. It requires coordination, integration, cooperation and collaboration with the structures of the defense system because the Army is not the bearer of defense against non-military challenges and threats.

In addition to their traditional roles in national defense and security, reserve forces can also contribute to intelligence collection and cybersecurity operations. One direction is the increased use of technology and automation to improve the capabilities of reserve units. For example, unmanned aerial vehicles and other autonomous systems can be used to increase the capabilities of reserve units, as individuals with expertise acquired from civilian life in these areas will be able to provide critical support and intelligence collection in various military operations. The second direction is the increased integration of reserve forces in cyber defense and cybersecurity operations.

Cybersecurity is becoming an increasingly important component of national defense and security, and reservists with expertise in this area could be used to enhance the military's capabilities in this area. This could include using reservists to provide

specialized training and support to regular military personnel, as well as deploying reservists to critical cybersecurity roles in times of crisis or war. As modern warfare increasingly relies on information technology and other forms of digital communication, the need for qualified personnel in these areas is growing. Reserve forces can help fill this gap, providing critical support to military and intelligence agencies in areas such as cyber defense, intelligence, and electronic warfare.

We have seen that in relation to the physiognomy of modern armed conflicts, the size of the territory, demographic potential, membership in international alliances, the composition and strength of the armed forces, national security strategies and defense strategies, all states, even those with neutral status, dimension their reserve forces differently and assign them different roles and missions. The specific tasks do not differ much from those performed by active forces and range from support and participation in operations, participation in peacetime operations, through bilateral military cooperation activities, capacity building and training of partner armed forces, specialist training, training for humanitarian operations, etc. Reserve military forces are made up of reserve personnel who perform tasks in exactly the same way as the active force.

It can also be concluded that it is an increasingly common practice in developed European countries to train and exercise reserves for tasks of providing assistance and protecting citizens in peacetime (for example, natural disasters, etc.) in cooperation with civilian structures. We can also point out that reserve military forces are intended to strengthen the existing military capacities of the armed forces and are engaged in the execution of missions and tasks of the armed forces, both on national territory and in external operations. In some European countries, reserve units within the Armed Forces are mainly intended to fill the composition with critical specialties (such as the specialties of Armored Units, chemical, biological and atomic weapons, intelligence and reconnaissance teams, elements of logistical support and segments for saving lives and protecting people's health).

What is happening with Serbia, a country that proclaims military neutrality, regarding the solution of the reserve component in its armed forces at this time?

According to the current concept of total defense, in an armed conflict with an unfavorable balance of forces for the Serbian Armed Forces, the Army will avoid direct conflict with the enemy's main forces, striving to skillfully, simultaneously and in a coordinated manner use its own forces in spatial and temporal conditions that the enemy least expects, i.e. it will apply an asymmetric approach. The grouping of forces and their combat deployment should enable coordinated strikes throughout the depth of the enemy's deployment in order to change the conditions and balance of forces and protect its own capabilities for the continuation of operations. The continuity of active operations is an important feature and guarantee of successful warfare. The use of reserve military forces organized into smaller units of company or battalion composition on a territorial basis would be a good solution for quick and sudden strikes deep into the enemy's de-

ployment. In cooperation with territorial defense units (if the concept of total defense were fully implemented) that would be formed from reserve members, reserve military forces would provide the ability to successfully wage war, but they would also play an important role in the strategy of deterring a potential aggressor from armed conflict.

In accordance with the concept of total defense, in a conflict against irregular forces, the use of reserve military forces of the Serbian Armed Forces implies the protection of the civilian population and important facilities in the territory from the actions of irregular forces, building trust between the local population and the authorities and one's own forces, and preserving freedom of movement in the zone and protecting one's own people, sources and supply lines, while active units would participate in finding, isolating irregular forces and taking decisive action against them.

We can conclude that in accordance with the needs and capabilities of the Republic of Serbia and the determination to provide a response to future challenges, risks and threats, reserve military forces should be developed so that:

- they are capable of active and preventive action and are a factor of deterrence against possible aggression;
- they contribute to strengthening the overall security, trust and stability of the Republic of Serbia;
- they represent a significant factor in the power of the Serbian Armed Forces;
- they develop the potential to adapt their capabilities to new security risks and threats;
- commands and units are interoperable to the necessary extent with active-duty units.

By the decision of the National Assembly of the Republic of Serbia of 15 December 2010, the obligation to serve military service was suspended as of 1 January 2011 and a professional army was established, thereby reducing the capabilities of persons in the reserve force. After the entry into force of the aforementioned decision, conscription into the Serbian Armed Forces is carried out on a voluntary basis, and persons who do not wish to voluntarily serve military service with weapons in the Serbian Armed Forces are subject to the obligation of entering into military records and the obligation to serve in the reserve force. The biggest problem arose in the composition and level of capabilities of the reserve force. The active reserve never took root in commands, units and institutions, while it was supposed to provide additional human resources, which would enable reliable and more efficient filling of units with motivated and trained personnel. Members of the passive reserve were very rarely called up for exercises, which further distances them from the army and makes them less usable. It is these people who would, if necessary, fill the Territorial Forces of the Serbian Army.

In accordance with the reserve training plans, the training of reserve personnel in this category began in 2019, but after the completion of basic military training in 2019, due to the COVID-19 pandemic in 2020, the training was suspended. Persons who invoked conscientious objection were not referred to training, but were instead assigned to civil protection units.

If the average number of high school graduates in Serbia is taken as a benchmark, the reserve personnel "lost" between 250,000 and 300,000 potential reservists in the period since compulsory military service was suspended. Given that the minimum needs for rejuvenating the deployed reserve force in the war units of the Serbian Armed Forces are around 5,000 people per year, in the past 10 years, during voluntary military service, there has been a significant decrease and deterioration in the age structure of the reserve force. The average Serbian reservist is 10-15 years older than his equivalent from half a century ago and in 99 percent of cases has had no contact with the army since completing his military service. A comparative review shows a decrease in the number of reserve forces up to the age of 35, while at the same time the number of deployed persons older than 45 has increased. With the introduction of a professional army, not only the passive but also the active reserve has been completely neglected, and the normal functioning of the active force of the Serbian Armed Forces has also been called into question.

The contemporary challenges, risks and threats that the Republic of Serbia faces are reflected in the following: extremism with elements of terrorism, all forms of organized crime, ethnic and national intolerance, unfair competition in the field of economy, integration into European security structures, population migration (especially from the territories of the Middle East and Africa), the Republic of Serbia's commitment to military neutrality, natural disasters and technical and technological accidents (Strategija nacionalne bezbednosti RS, 2009). The challenges and threats that the Republic of Serbia faces are the starting parameters for analyzing the capabilities of the Serbian Armed Forces, as well as its reserve components, and represent a prerequisite for proposing capabilities that should be developed in the conditions of modern conflicts. Of course, the capabilities of the reserve military forces and the Serbian Armed Forces need to be developed in the direction of future wars, the characteristics and nature of which are not difficult to guess.

CONCLUSION

From all the above, we can draw several conclusions that we have reached by researching this topic:

The reserve component of the defense forces of countries around the world essentially consists of military personnel who are not required to serve continuously on a full-time basis, except in the case of mandatory mobilization, which is usually reserved for the defense of the state. The use of reserve forces varies significantly between countries. In some countries, the mobilization and use of reserve military forces is limited to national defense. In others, it is available for responding to domestic natural disasters. In still others, it is required for expeditionary operations, etc.

The conclusion that large conscript armies, such as those of the Cold War, will no longer be needed has proven to be wrong. The physiognomy of conflict is changing,

and the conflicts that have been fought in the last 30 years (Yugoslavia, Iraq, Libya, Afghanistan, Syria...) have taken on specific forms and parameters that have implied that the activity of reserve forces in the conflicting parties was extremely frequent, necessary, and even indispensable. The current war in Ukraine is proof of this, where both sides have been forced to engage their reserve military forces, in addition to professional armies and various private mercenaries. And great powers, such as America and Great Britain, are increasingly counting on the capabilities and use of their reserve military forces, regardless of the architecture of the armed conflict in Ukraine. One could even conclude that the situation in which a large number of countries have switched to a professional army can be considered a trend that is slowly passing. Well-integrated, appropriately purposeful, motivated and ready reserve forces provide an extraordinary strategic opportunity to expand current military capabilities at a very low cost.

From the experiences of states that build their strategic orientation on the foundations of military neutrality, it is clear that they base their defense policy on the concept of total defense. Although they have not participated in modern conflicts, these countries must develop many factors for such a defense policy: first of all, a defense strategy and doctrine based on their own national defense capacities, their own defense industry (which must, to the greatest extent possible, meet the needs of the armed forces), strong armed forces (as a reliable factor of deterrence against armed aggression), a numerically respectable and trained reserve force, the development of which requires a stable recruitment system for replenishing the armed forces and an improved civil defense system. Ultimately, and at the very foundation of this defense policy, regarding the reserve component, which cannot be formed without recruits (soldiers with completed military service) and which cannot be trained for army missions without integration with the permanent composition, that is, without elaborated cooperation and collaboration with civil defense units, is the strong awareness of citizens about the need for state defense.

The concept of total defense and the approach to voluntary military service in Serbia are definitely incompatible commitments. The Serbian Army with its permanent composition (professional army) does not have the necessary and sufficient capabilities to respond to the tasks of the missions assigned to it. Strong, rejuvenated and trained reserve forces are needed. A large and strong, motivated army implies a higher percentage of reserve personnel, which, in conjunction with a developed civil defense system, represents a strong deterrent to any potential aggressor.

If Serbia wants to be perceived as a serious militarily neutral state, it must have respectable military forces that will ensure its smooth functioning (the principle of military self-sufficiency). This means opening up many significant issues for the country's defense, such as redefining key security documents, awakening citizens' moral awareness of patriotism, as well as strengthening and training its reserve component through the introduction of regular military conscription.

REFERENCE LIST

- Jokić, Ž. (2020). *Problem primene koncepta totalne odbrane u Republici Srbiji* (seminarski rad), Beograd: Univerzitet odbrane.
- Sretenović, M. (2007). Promenljivost fizionomije rata, *Vojno delo*, 2011, No. 1.
- Smith, R. (2008). *The Utility of Force: The Art of War in the Modern World*, New York: Knopf Doubleday Publishing Group.
- Lind, W. S., Nightengale, K., Schmitt, J.F., Sutton, J.W. & Wilson, G. I. (1989). *The Changing Face of War: Into the Fourth Generation*, Marine Corps Gazette (pre-1994); Oct 1989; 73, 10. ProQuest Direct Complete.

Documents

- Strategija nacionalne bezbednosti Republike Srbije*, Beograd, 2009.
- Strategija ONO i DSZ*, Savezni sekretarijat za narodnu odbranu, Beograd, 1987.

Internet sources

- Docslib. "Deterring Terror: Deterring Terror How Israel Confronts the Next Generation of Threats How Israel Confronts the Next Generation of Threats", n.d. <https://docslib.org/doc/5384274/deterring-terror-deterring-terror-how-israel-confronts-the-next-generation-of-threats-how-israel-confronts-the-next-generation-of-threats>.
- Levinson, Tom. "Israelis Don't Turn up for Reserve Duty, and the Consequences Could Be 'Catastrophic' ". Haaretz.Com, July 14, 2022. <https://www.haaretz.com/israel-news/2022-07-14/ty-article-magazine/.highlight/israelis-dont-turn-up-for-reserve-duty-and-the-consequences-could-be-catastrophic/00000181-fc83-db23-abf7-fce3ff750000>.
- Ministry of Defence. "Future Soldier: Transforming the British Army." GOV.UK, November 25, 2021. <https://www.gov.uk/government/publications/future-soldier-transforming-the-british-army>.
- Perry, Walt L., Richard E. Darilek, Laurinda L. Rohn, and Jerry M. Sollinger. *Operation Iraqi Freedom: Decisive War, Elusive Peace*. Rand Corporation, 2015.
- "National Reserve Forces Committee (NRFC) : NATO's ACT," n.d. <https://www.act.nato.int/nrhc>.

*Emilia Alaverdov*¹
*Nino Bochorishvili*²
*Zurabi Tchabashvili*³

THE IMPACT OF ILLEGAL MIGRATION ON TRAFFICKING AND ORGANIZED CRIME

Abstract

The problem of illegal migration is becoming increasingly acute, as it harms the economy and society. On the one hand, illegal migration makes it possible to eliminate the consequences of the demographic crisis; on the other hand, it can cause negative consequences of a social, political, economic, ethnic, and interpersonal nature. The main reason for the existence of illegal migration is the inequality in the economic development of the states. Migrants from less developed countries are attracted by high wages and high living standards. At the same time, there are other reasons as well, for instance war, natural cataclysms, etc. Illegal migration poses many challenges for the countries of origin, transit, and destination, as well as for the migrants themselves. Illegal migrants are particularly vulnerable to discrimination, exploitation, and violence. Illegal migrants are also at risk of exploitation by criminal organizations involved in human trafficking and migrant smuggling – criminal activities that constitute serious violations of the victims' human rights. In examining the current legal and policy framework, trafficking in persons draws on two key outcomes of the Office of the United Nations High Commissioner for Human Rights (OHCHR): the 2002 Recommended Principles and Guidelines on Human Rights and Trafficking and its extensive commentary.

Keywords: *discrimination, religion, hate speech, Europe, migrations.*

INTRODUCTION

The relevance of the work is determined by the fact that the presented issue is the result of modern world politics, which affects almost all countries of the modern world and their population. This is because migration has a great impact on both the country of origin and the host country, as well as the social circles and communities living there. It should be noted that there is an important connection between migration and community development and between migration and human trafficking. In this re-

¹ Georgian Technical University, Tbilisi, Georgia, alaverdovemilia@gmail.com

² Georgian Technical University, Tbilisi, Georgia

³ Georgian American University, Tbilisi, Georgia

gard, several agreements, declarations, and programs have been developed and approved by UN member states, the most important of which are:

- New York Declaration for Refugees and Migrants (2016), (UN General Assembly, 2016), which is based on various supporting human rights instruments, most notably the Universal Declaration of Human Rights (UN, 1948);
- International Covenant on Civil and Political Rights (OHCHR, 1966);
- International Covenant on Economic, Social, and Cultural Rights (OHCHR, 1966).

Another important document is the Global Agreement for Safe, Orderly, and Regular Migration, which was approved by the UN General Assembly on December 19, 2018, and entered into force on January 11, 2019.

Generally, international migrants can be divided into several main categories:

- Legally arrived migrants who are subsequently provided with work and occupy a place in the labor market;
- Migrant workers or contract workers who are accepted by countries in which there is a demand for foreign labor;
- Illegal migrants, including labor migrants, who usually occupy the lowest level of the labor market hierarchy;
- Asylum seekers for political or other reasons (UNHCR, 2015).

In examining the current legal and policy framework, trafficking in persons draws on two key outcomes of the Office of the United Nations High Commissioner for Human Rights (OHCHR): the 2002 Recommended Principles and Guidelines on Human Rights and Trafficking and its extensive commentary. Illegal migration is the movement of citizens and stateless persons of a foreign country, which involves entry or exit to one or another country, stay and employment in its territory, which is carried out in violation of the legislation that regulates the rules of entry, stay, transit and departure of citizens of a foreign country.

The Essence and Notion of Illegal Migration

Unfortunately, in the context of globalization in modern society, people have not only progressed but face discrimination and become victims of criminal activities. Along with globalization, transnational organized crime is growing, as criminal communities use economic, political, and cultural rapprochement and the emergence of new connections to achieve their goals. This is also facilitated by the new opportunities provided by information technology. Among other problems, in the period of globalization, the problem of human trafficking is alarming. The issue of human trafficking is considered the slavery of the 21st century. It is often also called "slavery of our days" because in both cases a person is considered only as a tool. The problem of human trafficking has become a subject of concern for all civilized humanity. Even though more and more countries are joining forces

to combat this phenomenon, modern slavery continues to be a harsh reality of our day.

Nowadays, crimes such as human trafficking and other forms of exploitation know no borders and occur in both rich and poor countries, causing such severe physical, psychological, or economic damage to their victims that their rehabilitation and return to society as full citizens require additional effort and time. Human trafficking is an organized transnational crime, and many countries unite to fight against it. Effective measures to prevent trafficking, especially the exploitation of women and children, require a comprehensive approach at the international level in countries of origin, transit, and destination, which includes measures aimed at preventing this phenomenon, punishing criminals, and protecting their victims, including through ensuring universally recognized human rights.

The problem of illegal migration is becoming increasingly acute because it has contradictory effects on the economy and society. On the one hand, illegal migration makes it possible to eliminate the consequences of the demographic crisis, on the other hand, it can cause negative consequences of a social, political, economic, ethnic, and interpersonal nature (Zubiashvili, 1999). The main reason for the existence of illegal migration is the inequality in the economic development of the states. Migrants from less developed countries are attracted by high wages and high living standards.

Another reason for illegal migration is the state's restrictive migration policy. Depending on the degree of influence of the flow of migrants on the socio-economic situation of the country, the state can create an "open door" regime or apply strict restrictive measures.

Two elements of illegal migration should be distinguished:

- a) Illegal entry into the country, which refers to the illegal entry of foreign nationals or stateless persons into the territory of the country, which is carried out in violation of the border crossing procedure or with false or incorrect documents;
- b) Illegal presence in the country; illegal presence in the country means the absence of residence or the expiration of the visa period (Frigo, 2015).

Irregular migration poses many challenges to countries of origin, transit, and destination, as well as to the migrants themselves. Illegal migrants are particularly vulnerable to discrimination, exploitation, and violence. Illegal migrants are also at risk of exploitation by criminal organizations involved in human trafficking and migrant smuggling – criminal activities that constitute serious violations of the victims' human rights (UN, 2013).

Despite the protection granted by international law, refugees and asylum seekers also face many difficulties in the migration process. Especially since the process of obtaining refugee status is becoming more and more complicated and it is becoming more and more difficult to find countries willing to accept refugees. The types of illegal migration are human trafficking, illegal crossing of the border, illegal transfer of a person across the border (smuggling), and staying in the territory of the country after the expiration of the legal stay. With a prior agreement and in exchange for a certain amount of money,

criminal gangs smuggle migrants across the border into countries where they have neither citizenship nor legal entry documents. In such cases, the relationship between criminal groups and migrants ends as soon as they cross the border. However, due to their illegal status in a foreign country, these migrants can easily become dependent on the people who helped them smuggle them into the foreign country. Criminal gangs often take advantage of such a situation and force migrants to work without any pay and thus cover the costs that smugglers spend on their transportation. It is important to note that "illegality" refers to a person's status at a certain point in time or during a certain period, not a person. For example, migrants fleeing conflict and persecution in their home countries and seeking protection in another country may be considered illegal migrants now at the border crossing, but their status may become legal once they claim asylum (Chkopoia, et al., 2023).

In addition, migrants with a legal status in the country may become illegal after the expiration of their visa or permission to stay in the country. The main actors of migration policy are usually nation-states. Contemporary migration policies are generally "restraining" and restrictive rather than attractive and liberal. To limit migration, states determine who can enter the country and under what conditions. There are certain categories of migrants based on their entry status: visa-free; short-term tourist or business visa; work visa; educational; marriage; or the purpose of a long stay in the host country.

At the same time, states determine who can stay in the country and how long:

- ▶ These may be categories of migrants that correspond to categories of entry, but very often there are differences: illegal entrants can claim asylum and legalize their presence if their claim is granted;
- ▶ Migrants could live illegally, but later legalized;
- ▶ Migrants are classified according to entry visa types, while the reasons for migration are more complex and may differ from visa typology. For example, a political refugee migrant tries to enter and stay in a country as an asylum seeker for this very reason, but the choice of country may be motivated by family or economic reasons.

As for the typologies of illegal migration, the most important thing here is to determine which parameter determines the illegal status: it is illegal to travel, enter, stay, or work in the receiving country, while the legal character of migration is determined by the law and policy, which determines the legislative procedures:

- ▶ What is legal in one country may be illegal in another;
- ▶ What is legal in a particular period, may be illegal in another period;
- ▶ The typology of legal or illegal entry depends on the possibilities of legal entry, the way of defining the categories of migrants and the mechanisms of entry, and, finally, the conditions of their use.

Human Trafficking and Human Rights

Migration and people smuggling have a common starting point – both migration and smuggling are done by the will of the person concerned. The difference is that migration is regular, but smuggling is not, so it can be seen as undermining the phenomenon of travel and therefore migration (IOM, 2020).

Human trafficking is considered a modern form of slavery in which people are tricked, coerced, threatened, or otherwise abused, which is contrary to human rights violations – victims of trafficking have limited independence, freedom of movement, and choice and are subjected to physical, psychological, or sexual abuse (OHCHR, 2014).

Among the most common forms of human trafficking are:

- ▶ Trafficking of women and children for sexual exploitation;
- ▶ Forced labor in agriculture, construction, household, and other sectors;
- ▶ Trafficking in human organs (Meskhi, 2014).

Trafficking is mostly assumed as a situation where people occur due to certain circumstances and reasons. For instance, they may be economic reasons, or just for their unwariness or unawareness. Trafficking can arise in any country or can include border crossing movements. Trafficking happens due to various reasons such as compulsory and exploitative labor in farms, factories, or even forced marriage, and forced intercourse. In examining the current legal and policy framework, human trafficking draws on two key outcomes of the Office of the United Nations High Commissioner for Human Rights (OHCHR): the 2002 Recommended Principles and Guidelines on Human Rights and Trafficking and its extensive commentary (OHCHR, 2011).

The Fact Sheet is divided into four chapters:

- Chapter One studies the essence and explanation of trafficking and its main features;
- Chapter Two discusses trafficking and human rights relations. It analyses human rights of those affected by trafficking and contemplates the current situation of particular people in the frame of human rights;
- Chapter Three deals with the commitments of countries. It points out the origin of these commitments and clarifies the legal responsibilities of the states in case of any damage or harm; it doesn't matter whether the state has taken responsibility or not; victim support and protection, repatriation, and medical facilities are discussed; also criminal law responses; prevention;
- Chapter Four examines the implementations and monitoring of the taken obligations ensuring that States, organizations, and societies are brought to justice for their actions and exclusion (Isaac, 2023).

International agreement about "human trafficking" is a very new concept. In fact, at the end of 1990s, states became concerned about trafficking since the case of illegal migration led directly to organized crime and trafficking. Thus the states started to meas-

ure its definition. The initially stated definition of trafficking was included in the 2000 Protocol to Prevent, Suppress, and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (OHCHR, 2000). It set the ground for such policy instruments as national laws.

The Trafficking Protocol defines the term "trafficking in persons" as follows:

a) Trafficking in persons" means the recruitment, transportation, transfer, harboring, or receiving of persons through the threat or use of force or other forms of coercion, kidnapping, fraud, deception, or violence. Giving or receiving a position of power or vulnerability or payments or benefits to another person to obtain the consent of the person under control for exploitation;

b) The consent of the victim of trafficking in persons to the intended exploitation provided for in subsection (a) of this article shall be irrelevant when any of the means listed in subsection (a) is used. Therefore, the three main elements that must exist for a situation of human (adult) trafficking to exist are: 1. Action, which means employment; 2. Threat; 3. Purpose can be exploitation (OHCHR, 2014).

Human trafficking and illegal border crossing is the second largest criminal industry in the world and is run by large international criminal networks (Alaverdov, et al., 2019).

It should be noted that illegal status is associated with increased risks to the physical security and personal freedom of a person. In addition, those present illegally cannot benefit from health, education, and other public/social services available to legal status holders (Gvenetadze, 2017).

The above risks can be avoided only by maintaining legal status abroad and legal migration. As a rule, the living conditions of illegal migrants are poor. They often cannot afford to rent a decent apartment, and those who agree to provide housing for illegal migrants usually offer housing in dangerous areas with unsatisfactory housing and low-security conditions (Alaverdov, 2021).

Prevention Mechanisms of Human Trafficking

The prevention mechanisms are directly connected and depend on the awareness of the issue. The study of associated factors allows potential victims to understand certain manipulative mechanisms of influence used by recruiters, which enables them to protect themselves from trafficking. In this case, it is worth mentioning some common factors contributing to human trafficking:

- Economic globalization;
- Economic and legal inequality of countries and regions;
- The possibility of transplanting human organs and tissues as a result of the development of science and, in particular, medicine;
- Victim behavior.

A new century, or a millennium, is not only a new timeline but a new milestone in the development of civilization, a distinctive feature that has become globalization and the unprecedented growth of information and communication technologies. In the context of globalization of the modern world, not only the fruits of progress and achievements of mankind have become common, but also the problems that society faces: human trafficking, exploitation, violence, drug use and distribution among minors and youth, natural and man-made disasters, information wars, uncontrollability of information streams, etc. Human trafficking is one of the most pressing problems of modern society and is of concern to the entire civilized world. Prevention of human trafficking involves both national measures (economic, social, ideological, legal, and educational) and special measures assigned to law enforcement agencies.

There are some certain measures to prevent human trafficking:

- carrying out legal, explanatory, and propaganda
- campaigns among the population,
- timely identification and elimination of trafficking in persons or related factors,
- intensification of operational search activities on identifying the perpetrators and victims and eliminating shortcomings in the fight against human trafficking,
- involvement of society and police in the fight against trafficking.

International Organization for Migration (IOM) is tightly cooperating with governments and non-governmental organizations through the implementation of different programs striving to strengthen the capacity of both governments and civil society institutions to address the problem more effectively.

Considering the nature of human trafficking as a phenomenon, its features, and specificity, it should be noted that the effectiveness of the fight against it is largely due to successful cooperation, which is enshrined in the Council of Europe Convention on Action against Trafficking in Human Beings. According to the provisions of the convention, cooperation is considered in two aspects: international cooperation and cooperation with civil society. In the field of international cooperation, the member states of the Council of Europe undertake to cooperate, applying the relevant international and regional instruments and implementing agreements based on legislation providing for common or mutual obligations. Cooperation implies the development of interstate programs and integrated approaches, common recommendations on migration, and implementation of concerted actions in this area.

International law is clear that asylum claimers must be assessed on their merits and not limited to determining how the applicant entered the country. In practical terms, this means that everyone, including smuggled migrants and victims of trafficking, should be given the full opportunity (including by providing adequate information) to apply for asylum or otherwise justify remaining in the country of destination on this basis. Many countries have penalties for illegal entry into the country, use of false travel documents, etc. It was noted that such punishments are increasingly expressed in the denial of the right to obtain refugee status.

CONCLUSION

Human trafficking is one of those crimes that requires, first of all, the tolerance of society to combat, and the interests of the victim should be put at the forefront. To do this, it is necessary to ensure the protection of the rights and interests of persons who have become victims of this phenomenon. In the field of combating human trafficking, we have to highlight the role of the International Migration Organization, which directly assists victims of trafficking. Through a network of offices in different countries, it fulfills the identification and repatriation of victims of trafficking. In this case, we have to mention the European Convention against Trafficking in Human Beings which has a relatively complex monitoring mechanism, including a Group of Experts on Action against Trafficking in Human Beings. The international human rights system plays a crucial role in combating such a violent phenomenon as trafficking and human victimization. Trafficking is considered one of the key topics of the modern world since it violates human rights and is against the Human Rights Act which states that a human being is granted freedom from his/her birth, and no one has the right to refrain from them. Even though the United Nations Human Rights Council pays great attention to the trafficking and along with the General Assembly regularly adopts resolutions on the issue, human rights are still under threat.

REFERENCE LIST

- Alaverdov, E. (2021). The Security Challenges of European Demographic and Politics Caused by Modern Migration Crisis. *Journal of Liberty and International Relations*, 31-42.
- Alaverdov, E., Pipia, S., Rusieshvili, E. (2019). The Impact of Modern Processes on the Modern World. In J. D. Sevda Akar, *Globalization, Poverty, Inequality, & Sustainability* (pp. 31-47). London: IJOPEC.
- Chkopoia, S., Alaverdov, T., Masaberidze, B. (2003). Outcomes of Conflicts, International Migration Processes, and Their Impact on the State Security and Social Wellbeing. In M. W. Emilia Alaverdov, *Handbook of Research on the Regulation of the Modern Global Migration and Economic Crisis* (pp. 122-138). Hershey: IGI Global.
- Friego, M. (2015). *Migration and International Human Rights Law*. Geneva: International Commission of Jurists.
- Gvenetadze, E. (2017). *The Aspects of International Security*. Tbilisi: Legal World.
- Isaac, O. (2023). *Irregular Migration A Case Study of Third-country Nationals in Sweden*. Malmo: Malmo University.
- International Organization for Migration. (2020). *World Migration Report 2020*. Geneva: IOM.

Meskhi, M. (2014). *Legal Aspect of Trafficking, the Methods of Combating it, Experience and Perspective*. Tbilisi: Tbilisi State University.

Office of the United Nations High Commissioner for Human Rights. (2011, February 01). *Recommended Principles and Guidelines on Human Rights and Human Trafficking: Commentary*. Retrieved from <https://www.ohchr.org/en/publications/reference-publications/recommended-principles-and-guidelines-human-rights-and-human-0>

Office of the United Nations High Commissioner for Human Rights. (2014). *Human Rights and Human Trafficking*. Geneva: OHCHR.

Office of the United Nations High Commissioner for Human Rights. (2000, November 15). *Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime*. Retrieved from <https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-prevent-suppress-and-punish-trafficking-persons>

United Nations General Assembly. (2016, September 19). 71/1. *New York Declaration for Refugees and Migrants*. Retrieved from https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_71_1.pdf

United Nations Human Rights Office of the High Commissioner. (1966, December 16). *International Covenant on Civil and Political Rights*. Retrieved from <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

United Nations. (2013). International Migration Policies. In *U. Nations, Irregular migration, human trafficking and refugees* (pp. 91-99). New York: UN.

United Nations Refugee Agency. (2015). *Global Report 2015*. Retrieved from https://reporting.unhcr.org/sites/default/files/GR_2015_Eng.pdf

Zubiashvili, T. (1999). *Modern International Migration*. Tbilisi: Tbilisi State University.

Galit M. Ben¹

THE CHANGING NATURE OF ARMED CONFLICTS IN THE 21ST CENTURY

Abstract

This study examines the evolving nature of armed conflicts in the 21st century, focusing on the resurgence of large-scale interstate wars and the transformation of non-state actors into formidable military forces. Through comparative analysis of the Russo-Ukrainian War (2022-present) and the Israel-Hamas War (2023-present), we investigate how modern warfare blends conventional and asymmetric elements. Our findings indicate a shift from the era of "small wars" to a new paradigm where terrorist organizations like Hamas demonstrate capabilities rivaling state armies. The research highlights the critical role of innovative, low-cost technologies such as drones and cyber warfare in reshaping battlefield dynamics. We argue that traditional distinctions between state and non-state actors in warfare are increasingly blurred, necessitating a reevaluation of military doctrine and international security frameworks. This study contributes to the understanding of contemporary armed conflicts and their implications for global security, military strategy, and international relations in an increasingly complex geopolitical landscape.

Keywords: *armed conflicts, asymmetric warfare, 2023 Hamas-led attack on Israel, 2023 Israel–Hamas war, Russo-Ukrainian War, unmanned aerial vehicles (UAV), drones.*

INTRODUCTION

Nowadays, we live in a post-modern historical era. Almost no trace of the "old order" of things left. We thought that the era of the Great War was over. World War I (1914-1918) and World War II (1939-1945) were behind us. There have been no significant wars since the Yom Kippur War (1973), the Iran-Iraq War (1980-1988), and the Yugoslav War (1991-1995). At the end of the 20th century, there were still "post-imperial" wars like the occupation of Afghanistan by the USSR in the seventies, or the occupation of Iraq by the U.S. (1991, 2003) and the occupation of Afghanistan by the U.S. (2001), but the significant/ national wars were over.

Twenty years ago, around the millennium, we entered an era of "small wars" (asymmetric wars) according to politicians, the military, the media, and academic researchers from all over the world. It was an era in which militant armed groups such as Hezbollah in Lebanon, ISIS (the "Islamic State") in the Middle East (in large parts of

¹ Achva Academic College, Beer Tuvia, Israel

Syria and Iraq), Hamas in Gaza, Al-Qaeda in Afghanistan, Boko Haram in Nigeria, Abu Sayyaf in the Philippines, the Houthis in Yemen and more were fighting against modern armies of states like: the US army, the Israeli army, the Global Coalition against ISIS ("Operation Inherent Resolve"), the army of Saudi Arabia, etc.

It is important to note that wars between large armies did not characterize the "small wars" period. For example, it included hybrid conflicts such as suicide terrorism, missile attacks, and "lone wolf" terrorism (Hamas, Palestinian Islamic Jihad for example). Or it was taking hostages, murdering, and burning them alive (al-Qaeda, ISIS in Iraq, Syria, and Libya). There were terrorist attacks in European capitals, American cities, Israeli cities, and towns in Middle Eastern and Asian countries such as Iraq, Syria, Afghanistan, Pakistan, etc. The hybrid era also included Russia's annexation of Crimea (an area of sovereign Ukraine) in 2014.

During the last two decades, more attacks and wars have taken place inside cities than on battlefields. Consequently, most of the victims were and are innocent civilians lacking knowledge, experience, and combat training. Around the world, city squares, educational and cultural institutions, entertainment venues, and cafes have become battlefields. Mary Kaldor use the term "New Wars" as opposed to "Old Wars" (the idea of war that predominated in the nineteenth and twentieth centuries). "New Wars" are the wars of the era of globalization. Typically, they take place in areas where authoritarian states have been greatly weakened (Iraq, Afghanistan, Gaza Strip, Syria, etc.). In such contexts, the distinction between state and non-state, public and private, external and internal, economic and political, and even war and peace are breaking down. Moreover, the breakdown of these binary distinctions is both a cause and a consequence of violence. In "New Wars" there is no distinction between combatants and non-combatants, and those who organized violent crime and terrorism blurred, so the main victims are civilians (Kaldor, 2012).

General Rupert Smith defined in 2005 that "war no longer exists", that is, war as "battle in a field between men and machinery" or "a massive deciding event in a dispute in international affairs" is unlikely to happen again. Smith characterized that the world is experiencing a new paradigm of war in the late 20 and early 21 centuries. It's "war amongst the people", in which nebulous, open-ended conflicts have become the norm. Industrialized armies, according to Smith can't win "wars amongst the people", as used to be in the past. "Wars between the people" are complex and nonlinear and do not differentiate between frontline and home front (Smith, 2005).

After all written above about the age of "small wars", on February 24, 2022, war returned to be industrial-modern, and significant. Russian forces invaded Ukraine (Kirby, 2022), another sovereign nation ("Russian invasion of Ukraine 2022"). As a result, the world entered an era of bipolar doctrines (Russia, Iran, China and North Korea, versus U.S., European Union and NATO) (Carpenter, 2023). The war in Ukraine continues to this day. As another sign of the return of the "old war" genre, Hamas soldiers

(and Palestinian "civilians") invaded Israel on October 7, 2023 (Kingsley & Kershner, 2023). Additionally, there are still small wars being fought, such as the terrorist attack on Moscow on March 22, 2024, by ISIS-Khorsan, the 2023 Paris attack, or the Aras school stabbing (October 13, 2022) (Europol, 2024).

This study aims to map the new world of war emerging today and identify, define, and explain the latest types of battle field and armies. We aim to understand how war changes in a new and complex geopolitical era. In addition, we are re-examining what constitutes an army as terrorist/guerrilla groups have moved from terrorist organizations to army models (Hamas and Hezbollah for example).

Research hypotheses:

1. A new era of significant/ national wars/conflicts has begun.
2. War's paradigm is changing.
3. The definition of an army has changed.

Methods

The study is part of a broader comparative study of the Russo-Ukrainian war (beginning in February 2022), the 2023 Hamas-led attack on Israel and the 2023 Israel-Hamas war. In this study, we will compare the Russian invasion of Ukraine and the Russia-Ukraine war from February 2022 (ongoing) with the Hamas invasion of southern Israel (The October 7 massacre) and the Israel-Hamas war from October 2023 (ongoing). The research uses comparison table and artificial intelligence. We compare and contrast military capabilities, tactics, strategy, innovation, technology, weapons, and global implications, etc.

Case Studies:

1. Russo-Ukrainian War (February 24, 2022-present)
2. 2023 Hamas-led attack on Israel ("October 7")
3. 2023 Israel-Hamas war (October 7, 2023-present)

The Russo-Ukrainian War (February 24, 2022–present (

The ongoing Russo-Ukrainian war represents a significant shift from the era of "small wars" to the resurgence of large-scale interstate conflict. In 2014, Russia annexed Crimea, a territory within the sovereign borders of Ukraine, through military force. This initial invasion was viewed through the lens of "small wars" or limited regional conflicts. However, the full-scale invasion of Ukraine by Russian forces on February 24, 2022 marked a transformative moment, signaling the return of major conventional warfare between nation-states (Kagan et al., 2023).

This reference is from a respected think tank that provides regular assessments of the Russo-Ukrainian war. The specific date (February 24, 2023) is chosen as it marks

the one-year anniversary of the full-scale invasion, likely providing a comprehensive analysis of the conflict's nature and implications.

The motivations behind Russia's invasion are complex. President Vladimir Putin has cited preventing Ukraine from joining NATO and potentially changing the Ukrainian government as key objectives (Sabadus, 2022). However, the pretext provided was the defense of pro-Russian separatist regions against alleged "genocide" (BBC News, 2022). Some analysts suggest Putin aimed to significantly weaken Ukraine's military capabilities to diminish its resistance to Russian influence (Kofman et al., 2022).

Against initial expectations of a swift Russian victory, Ukraine mounted a robust defense. Most Western analysts predicted Ukraine would succumb within 72 hours (Kirby, 2022), but two years later, Russia has failed to establish control over the country. The tenacity of the Ukrainian resistance has defied assumptions about the superiority of Russia's "hybrid warfare" doctrine and conventional military strength.

Both sides have employed novel weapons systems. Russia has deployed autonomous combat vehicles, multipurpose robots for combat and logistics roles, and small robotic tanks (Bendett, 2022). Ukraine, in addition to receiving advanced missiles and aircraft from Western allies, has rapidly developed and manufactured its own drones, producing an estimated 50,000 per month (Atherton, 2022). These low-cost drones, capable of targeting armored vehicles, have proven devastatingly effective, with Ukraine claiming responsibility for destroying over 2,600 Russian tanks, nearly half by drones (Bendikaite, 2023).

The conflict has driven tactical innovation out of necessity, with Ukraine actively seeking to deny Russia the ability to replicate its asymmetric advantages. As Samuel Bendett, a military technology expert, observed, "Currently, if something moves on the battlefield, a drone sees it and hits it" (quoted in Atherton, 2022). The "drone army" and counter-drone strategies employed by Ukraine foreshadow the nature of future warfare. General Oleksandr Pavliuk, the commander of the Ground Forces of Ukraine said that the widespread use of drones has changed the tactics of battles in the Russo-Ukrainian war as drones are now more lethal than artillery and aviation, and tactics of the battlefield, and the infantry "settled deeper". "Drones are now killing more soldiers on both sides than anything else. Drones can see almost everything, not only on the front line, but also at a depth of 10 to 30 km on both sides" (Golovan, May 3, 2024). As things stand, neither Ukraine nor Russia can create a large strike group without being noticed and hit by long-range strike drones and artillery. Because of this, the armies can no longer move in battalions or even companies, he added. Now neither Ukraine nor Russia can create a large strike group without being noticed by enemy UAVs (Ibid).

The military capabilities employed by Russia and Ukraine in the current conflict highlight the juxtaposition of advanced conventional arms and asymmetric innovative systems. Russia has leveraged its modern mechanized forces, deploying main battle tanks like the T-72B3, T-80BVM, and T-90M (Bendett & Leed, 2022), complemented

by infantry fighting vehicles such as the BMP-3, BMP-2, and BTR-82A. Russia's formidable artillery assets range from truck-mounted Msta-S howitzers and 2S19 Msta-S self-propelled guns to multiple rocket launchers like the BM-30 Smerch (Bendett & Leed, 2022). Russian airpower has comprised attack helicopters such as the Ka-52 and fixed-wing aircraft like the Su-34 and Su-35 jets for airstrikes (Balmforth & Astakhova, 2022). Additionally, Russia has employed conventional and precision-guided missiles, including the Iskander ballistic missile, and electronic warfare systems like the truck-mounted Krasukha-4 for communications jamming (Bendett & Leed, 2022).

In contrast, Ukraine has relied on Western-supplied anti-tank weapons like the Javelin and NLAW to counter Russian armor (Atherton, 2022), while its artillery includes indigenous howitzers, U.S.-provided M777 towed howitzers, and HIMARS rocket systems. Ukraine's air defenses comprise man-portable Stingers and Soviet-era S-300 surface-to-air missile batteries (Bendett & Leed, 2022). Crucially, Ukraine has innovated with inexpensive reconnaissance and attack drones, such as the Turkish Bayraktar TB2, and loitering munitions, offsetting some of Russia's conventional advantages (Atherton, 2022). Ukraine's forces also continue to operate Soviet-designed tanks, infantry fighting vehicles, armored personnel carriers, and aircraft inherited after independence (Bendett & Leed, 2022).

In summary, Russia deployed its full array of conventional military capabilities, including state-of-the-art tanks, advanced jet fighters, sophisticated artillery systems, and cutting-edge electronic warfare equipment. However, Ukraine has successfully mitigated some of Russia's advantages through a combination of Western-supplied anti-tank weapons and artillery, coupled with innovative utilization of cost-effective drones and unmanned systems. This conflict has exposed both the formidable strengths and unexpected vulnerabilities of Russia's armed forces.

The state of Israel in the asymmetric era

Most of the early years of the existence of the State of Israel were accompanied by major wars like: The 1948 war, the 1967 war and the 1973 war.

The change started during the Second Lebanon War (2006). Then the missile range of Hezbollah rockets reached almost to the center of the Israeli state. During "Operation Pillar of Defense" (2012) and the "2014 Israel-Gaza conflict" (2014), the missiles of Hamas and Palestinian Islamic Jihad (PIJ) reached the Tel-Aviv area, the center of Israel. In addition, the Hezbollah also launched missiles from Lebanon to the northern part of Israel. Also, the radical Salafi terror organization "Ansar Bait al-Maqdis" (affiliated with al-Qaeda), launched rockets from Sinai Peninsula to the southern part of Israel. It created an aura of demoralization in the Israeli home front. (Ben-Israel 2018a, 54)

Furthermore, Hamas and the Palestinian Islamic Jihad organization were the first organizations to commit suicide terrorism against Israel on sovereign Israeli territory. Between 1993 and 2008, Hamas carried out a series of suicide attacks in Israel. In response, Israel built the West Bank barrier (2006-2002). After the Israelis built the Israeli West Bank barrier, Hamas and Palestinian Islamic Jihad increased their attacks significantly. This genre of attack was last perpetrated in 2008 (Ben-Israel & Shorer-Zeltser, 2012).

However, Palestinian terrorism is known from the late 60', for its innovation and entrepreneurship (Ben-Israel, 2008). Hamas and Palestinian Islamic Jihad, two Palestinian jihadist terrorist organizations, reinvented themselves by firing rockets at Israel. Since 2001, rocket attacks from Gaza into Israel have frequently used rocket artillery (shooting steep trajectory rockets). Rocket launches in Israel increased after 2008 (the end of the suicide terrorist genre). Israeli routines were constantly influenced by them, especially in the Gaza Envelope, but also in Tel Aviv (Rubin, 2011). Despite all the military operations of the modern military-industrial machine, the IDF (to name only the main ones: Operation Cast Lead, Operation Pillar of Cloud, and Operation Solid Cliff), Israel has been unable to prevent Hamas and the Palestinian Islamic Jihad from firing rockets at Israel (Eilam, 2014).

On October 7, 2023, Hamas destroyed the separation fence between Israel and Gaza strip. Cities and kibbutzim near the south border of Israel were occupied between 8-36 hours by Hamas army (Heller & Lubell, October 8, 2023). Hamas demonstrated the capabilities of an army on October 7. However, scholars like Hoffman, Scales & Ollivant noted before October 7, 2023, that both Hamas and Hezbollah possessed skilled soldiers and commanders, organized, elite units, anti-tank missiles, and intelligence capabilities. As difficult as compound wars have been, the operational fusion of conventional and irregular capabilities in hybrid conflicts may be even more complicated. Compound wars offered synergy and combinations at the strategic level, but not the complexity, fusion, and simultaneity we anticipate at the operational and even tactical levels in wars where one or both sides is blending and fusing the full range of methods and modes of conflict into the battlespace (suicide terrorism, missiles, kidnapping, targeting civilians and state army, etc.), such as Hezbollah in the Second Lebanon war in 2006. The latter effectively fused militia forces with highly trained fighters and antitank guided missile teams into the battle. Hezbollah clearly demonstrated the ability of no-state actors to study and deconstruct the vulnerabilities of Western-style militaries and devise appropriate countermeasures (Hoffman, 2009, 36-37).

Also, some observers of the transformation admit that Hezbollah now is among the most skilled light infantry on the planet. And now there is Hamas. Gone are the loose and fleeting groups of fighters seen during Operation Cast Lead in 2008. In Gaza they have been fighting in well-organized, tightly bound teams under the authority of connected, well-informed commanders. Units stand and fight from building hideouts and tunnel entrances. They wait for the Israelis to pass by before ambushing them from the rear, like Hezbollah and the Islamic State (Scales & Ollivant, 2014).

Since "October 7", Hamas is defined as an army for the following reasons. Firstly, Hamas considers itself a military organization. We may need to accept an organization's self-definition in a postmodern world. Most concepts in the world today have fluid definitions. Organizations, individuals, and groups must define themselves and how they see themselves. Hamas challenges the "Old World's" definition that look upon it as a terrorist organization or and a guerrilla group.

Secondly, Hamas has a foreign policy and deep and close ties with three powers: Qatar, Iran, and Russia. Qatar funded Hamas in Gaza with hundreds millions of dollars (Schanzer, 2018). Qatar, a tiny emirate, became the unflinching mediator for the release of the Israeli abducted from the October 7 massacre. Qatar pushed Egypt into a corner, and gained regional influence (Federman & Magdy, 2023). Before October 7, with signing agreements and providing funding for the United Nations organizations for approximately 500 million dollars, Qatar was one of the first countries to support the United Nations. The United Nations House, which several UN organizations will use, was also opened by Qatar. In this context, the Qatar Development Fund signed a multi-year donation agreement with UNRA (Aid Agency for Palestine Refugees) totaling \$18 million for 2023-2024, including Gaza. Qatar announced recently that it would continue to support an organization whose employees participated in the October 7 massacre and hid abducted children (Associated Press, 2024).

Also, before October 7, Qatar had prepared the Western world's infrastructure to support Hamas. Qatar's strategy has consistently been to "lubricate" crucial factors in the Western world so that it can sail along with its interests when the time comes. Hamas has a global virtual community as well as a global physical community. According to the NCRI Research Institute, a non-government organization based at Rutgers University in New Jersey, Qatar, Saudi Arabia, and the United Arab Emirates contributed at least \$4.4 billion to U.S. colleges between 2014 and 2019. Over \$5 billion has been donated by authoritarian Middle Eastern countries to American universities in the last five years, in addition to contributions from other Middle Eastern countries. The top five universities that benefited from these donations include Carnegie Mellon (Pittsburgh), Cornell (\$1.2 billion), Harvard (\$894 million), MIT (\$859 million), and A&M College Station in Texas, which received about half a billion dollars (Brumfield, 2023).

Hamas' strategic plan led to the largest demonstrations in history after the October 7 massacre. Demonstrations continue to this day. According to Dina Lisnyansky who is an expert on Islam in Europe, those behind the demonstrations in Europe are Iranian or pro-Hamas organizations. These organizations are often referred to as the BDS movement. Many of us mistakenly believe that the BDS movement is far removed from the hostile elements and terrorists we are familiar with in the Middle East. In Europe and the United States, this movement unites many organizations related to the global "Muslim Brotherhood" movement. The organizations that support these demonstrations, stand be-

hind them, and invite them to participate are organized and detailed. Since October 7, these demonstrations have grown considerably in Europe. Most of the protesters in Europe in the last six months are not Palestinians. There is no correlation between the size of the protest that may take place there and the fact that many people who don't necessarily identify with the Palestinian issue value it. Due to the large university, students are engaged in this issue and are the center of power in the story. The pro-Palestinian demonstrations are characterized by clear messages against Israel and its right to exist. They create the appropriate atmosphere and encourage the demonstrations (Lisnyansky, 2024).

Thirdly, Hamas had a military strategy, a combat theory, and a military strategy. October 7, 2023, brought all of this to fruition. Before the invasion of Israel, Hamas executed a brilliant diversionary operation by firing massive rockets into Israel (South, Shfela, and Gush Dan). According to IDF data released by the spokesman, approximately 3,000 launches were made against the country's territory in the first four hours of the war. Eight military outposts were taken over, weapons were destroyed, and military equipment was burned – disrupting IDF command, communication, and control. A diversionary operation was also conducted by infiltrating windsurfers and small sailing vessels, which simultaneously eased the wave of foot invasion through the separation fence (Katz, 2023).

In the early hours of October 7, 2023, Hamas conquered southern Israel. Hamas occupied military bases, cities (Sderot and Ofakim), kibbutzim, and moshavim. Some were abandoned after a few hours, and others held out against the IDF for up to 36 hours. For a limited period, Hamas was more successful in its invasion of Israel than any other Arab army ever during previous Israeli-Arab wars. Hamas captured 8 military bases in southern Israel, the Navy base, and Gaza Division bases, including the Erez crossing point (destroyed by Hamas) and the Nahal Oz post. Israeli soldiers were taken captive, were killed, murdered and butchered after captive and female Israeli soldiers were raped (UN Human Rights Office, 2023). In many ways, the acts of rape, cutting off organs, and burning people alive that took place on October 7 by Hamas warriors are entirely similar to the actions carried out by the ISIS organization in the Middle East. It happened "during the second half of 2014, the 'Islamic State' dominates a huge territory in northeastern Syria and western and northern Iraq" (Ben-Israel 2018b, 57).

The Israeli Gaza Division lost control of the outpost when thousands of Palestinians, some of them unarmed, spontaneously raided the surrounding kibbutzim and kidnapped Israeli citizens into Gaza. During the invasion, Hamas used a variety of military and diversionary tactics: at sea, in the air, on land, in cyberspace (to disrupt the technological measures near the separation wall). Hamas soldiers took videos of the invasion and occupation of the south of Israel with GoPro cameras. They broadcast simultaneously the films on Facebook and Telegram (Gross, 2023).

The Hamas fighting doctrine aims to simultaneously use a large number of suicide drones against military, civilian, and infrastructure targets near the border on com-

mand day. Additionally, Hamas may practice taking out low-altitude aircraft and sending them to Israel from the depths of the sea (Hecht, 2023). Hamas attempted to establish a unit of fighters using paragliders to infiltrate Israeli territory in the past. This unit may still exist, but it is unknown.

Using simple technological means, land raids, sea raids (over the water and submarines), and air raids are all possible. They are capable of blowing up tanks on their occupants with their UAVs. Tanks aren't needed. The only thing they need to do is destroy the IDF's tanks. In the new world of war, roles are reversed; the weak aggressor is somehow stronger than the conventional army he is attacking. Rather than artillery, the modern industrial army has a missile corps with upgraded rocket arrays. There are drones for collecting intelligence, and suicide drones. The whole array replaces the air force of the contemporary industrial army. RPGs, mines, and more are also available. There is evidence that Hamas has been training with advanced weapons for years, starting in 2014 and they had Iranian guides. The Hamas army is composed of many forces (soldiers and mob), an elite unit (the Nuh'ba), and a naval commando unit (its elite unit dives long distances in motorized vehicles). Hamas has a weapons production system based on Iranian and Syrian missiles. The improvements were made by increasing explosive materials and accuracy (using outdated means compared to Hezbollah's precision project), increasing rocket numbers, and improving existing models (Gross, 2024). Hamas continues to produce weapons in Judea Samaria and Gaza today. In the first weeks after the Israeli army invasion of Gaza, their creativity, innovation, boldness, and strategic military sophistication were also evident in their fighting against Israel. During the Gaza Strip conflict, the Hamas army engaged in three dimensions of combat: on the surface, in tunnels, and by firing missiles and attacking anti-aircraft guns (Marcus & Shuster, 2023).

In summary, Hamas has emerged as a young, innovative, and audacious military force, unburdened by the cumbersome bureaucracy typical of traditional armies. Unlike the Israeli military, Hamas can swiftly acquire resources such as drones from China without navigating complex bureaucratic channels. In today's digital and virtual landscape, nearly everything, including weaponry, can be substituted with cost-effective, simultaneous, and efficient alternatives.

The proliferation of online resources, such as YouTube tutorials on bomb assembly, has democratized access to dangerous knowledge. Furthermore, the ease of procuring inexpensive digital drones or weapon components from China through platforms like Amazon, often evading enemy detection, has revolutionized warfare logistics. Moreover, Hamas benefits from a pool of technologically skilled individuals (engineers) not only in the Gaza Strip and Palestinian Authority, but also in countries like Bangladesh, Pakistan, and Iran. These technologists, digital experts, and DIY (Do it yourself) enthusiasts form a formidable knowledge base for the organization.

In the aftermath of the October 7 attack, Hamas has demonstrated capabilities comparable to a state army. The organization boasts a comprehensive military structure, including: a) Well-defined strategy and tactics; b) An air force (comprising unmanned aerial vehicles and drones); c) Missiles and rockets that effectively replace traditional artillery; d) Electronic warfare capabilities; e) An advanced intelligence wing; f) Elite special forces (including the Nukhba unit); g) Technological support from Iran + Economic backing from Qatar; h) Global digital infrastructure. This multifaceted military apparatus underscores Hamas's evolution into a formidable fighting force, blurring the lines between non-state actors and conventional armies.

Comparing table: *the ongoing Russo-Ukrainian War and the 2023 Israel–Hamas war*

Criteria	Russo-Ukrainian War	2023 Israel–Hamas war
Period	February 24, 2022-present	October 7, 2023 - present
Nature of Conflict	Interstate war between sovereign nations (Russia vs. Ukraine).	Hamas' invasion of the south of Israel and the IDF's invasion of Gaza.
Objectives	The occupation of Ukraine and the installation of a puppet government on behalf of Russia.	Hamas: 1. First raid wave on Israel, which additional raid waves will follow. 2. Taking captive a large number of soldiers and men aged 17-50 in the first moments of the fighting and sending them to Gaza. 3. Taking over 221 settlements. It was Israel's goal to eradicate Hamas' military capabilities and Gaza's control.
The Reality	According to Putin and Western officials, the Ukrainian army would strengthen 72 hours after the Russian invasion and then surrender. After more than two years since the Russian invasion of Ukraine, the Ukrainian military and its citizens still successfully face the Russian army.	A Hamas invasion and occupation of southern Israel, including military bases. A series of events in Israel , including the expulsion of Hamas from Israeli territory, the release of Israeli hostages, and the occupation of Gaza Strip by Israeli troops.
Global Implications	Third World War's opening shot?	Second shot of the Third World War?
Parties Involved	NATO, U.S., The European Union from one side, and China, North Korea and Iran (by providing weapons to the Russian military) , from the other side.	Iran, China, North Korea, Russia, Turkey, Egypt, Qatar, Hezbollah, Houthis, the Shi'ite militia in Iraq and the Shi'ite militia in Syria, U.S.
Modern Industrial Army	The Russian army is a large industrial army. While the Ukrainian military is much smaller, the USA and other states have taken care to arm it.	Israel has a strong modern and post-modern army. Hamas does not have a heavy industrial army.

DIY, Drones	The Ukrainian army has an advantage over the Russian army when it comes to drones, gamers, unmanned vehicles, and DIY concept. However, the Russian army is closing the gap nowadays.	Hamas had a significant advantage over Israel on October 7 due to the drones and DIY equipment they used.
AI, Robots	Both sides likely employing AI for intelligence gathering and strategic planning, though specific capabilities are not fully public.	Especially Israel, but since Hamas is an Iranian proxy (cyber digital power), Israel is likely to be surprised.
Digital Arena (Hacktivism) + Information Warfare	<p>Both sides have seen support from independent hacker groups, with notable activities from groups like Anonymous supporting Ukraine.</p> <p>Information Warfare</p> <p>Russia: Extensive use of disinformation campaigns, leveraging social media and state-controlled media outlets.</p> <p>Ukraine: Effectively using social media for morale boosting, international support gathering, and countering Russian narratives.</p>	<p>In the digital arena, Hamas is a dominant force, with the support of Qatar and Iran, plus the "Muslim Brotherhood" branches in the U.S. and Europe.</p> <p>Information warfare:</p> <p>Both sides are actively using social media and online platforms for propaganda and to shape international opinion</p>
Cyber Attacks	<p>Russia: Known for sophisticated state-sponsored cyber operations, targeting Ukrainian infrastructure, government systems, and media</p> <p>Ukraine: Has shown improved cyber defense capabilities, and has also launched counter-attacks on Russian targets..</p>	<p>Hamas and affiliated groups:</p> <p>Attempted attacks on Israeli infrastructure, including water systems and power grids.</p> <p>Disinformation campaigns on social media platforms.</p> <p>Attempts to hack into Israeli military communications.</p> <p>Israel: Cyber operations targeting Hamas's command and control systems.</p> <p>Disruption of communication networks used by Hamas.</p> <p>Intelligence gathering through cyber means.</p> <p>Third-party actors:</p> <p>Various hacktivist groups have launched attacks supporting both sides.</p> <p>Increased phishing attempts and malware distribution leveraging the conflict.</p>

FINDINGS

The conflict has revealed parallels between the Russian and Israeli armies as large, modern forces facing asymmetric challenges. While initially at a disadvantage, the Ukrainian military rapidly adapted through Western support, including equipment, training, and innovative tactics and weaponry. In addition, both Israeli and Russian armies are sovereign, industrial, bureaucratic, and equipped with costly equipment, prepared for conventional warfare against similar forces.

Interestingly, Russia's invasion of Ukraine and Hamas's invasion of Israel caught both states completely off guard. The Russians were surprised by Ukraine's army, equipped with advanced yet inexpensive technological weapons, including drones, unmanned aerial vehicles (UAVs for attack, suicide missions, and intelligence gathering), robots, and AI. These digital, efficient, and cost-effective tools are easy to supply and transport. Ukrainian soldiers, some of them teenage gamers, astounded Russia's army with their proficiency in using suicide drones to attack Russian soldiers and tanks en masse.

Similarly, Israel was caught off guard by Hamas's excellent strategic and tactical invasion, as well as its use of simple weapons and digital technology, such as suicide drones and inexpensive drones for dropping explosives. The Hamas military also surprised the Israelis with vans armed with machine guns, shoulder-fired anti-aircraft missiles, and RPG rockets. Notably, both Hamas and the Russian armies are equipped with Iranian unmanned aerial vehicles (Shahed-136) and ballistic missiles.

SUMMARY

We live in a postmodern historical era where nearly everything has changed. The age of great wars seemed to have passed, and during the millennium, we entered an era of "small wars", characterized by asymmetric warfare between terrorist organizations (Hamas, Hezbollah, ISIS, etc.) and state armies. However, as of February 24, 2022, the landscape of armed conflicts in the 21st century shifted dramatically. The Russian army's invasion of Ukraine signaled a return to an era of national wars, potentially marking the beginning of a third world war. On October 7, 2023, the Hamas army's invasion of Israel and the subsequent 2023 Israel-Hamas war further reinforced this trend. These three armed conflicts significantly strengthen the research hypothesis that a new era of major national conflicts has begun.

Regarding the hypothesis that war's paradigm is changing: both Russia and Israel were surprised by a new type of army wielding novel weapons: cheap, efficient, light, digital, and technological. The unmanned aerial vehicles used by the Ukrainian and Hamas armies have forever altered the face of battle, both geographically and tactically. This shift has transformed the concept of war and redefined what constitutes an army in our era. An alternative air force has emerged: the drone corps. Today, Ukraine, Iran, Hamas, Hezbollah, and the Houthi movement in Yemen control these alternative air forces.

Since "October 7", Hamas can be defined as an army for several reasons. Primarily, Hamas considers itself a military organization and has demonstrated a sophisticated foreign affairs, diplomacy, and global propaganda doctrine. Hamas developed a military strategy, combat theory, and military tactics, which came to fruition on October 7, 2023. In the early hours of that day, Hamas conquered a large part of southern Israel. For a brief period, Hamas was more successful in its invasion of Israel than any other Arab army in previous Israeli-Arab wars.

The study results indicate that the era of significant wars has returned. Furthermore, the research finds that terrorist organizations, guerrillas, and armed militants have evolved into armies of terror. In many ways, these terrorist armies are now equivalent to state armies and must be treated as such.

REREFENCE LIST

Atherton, K. D. (2022, September 1). Ukraine's Inexpensive "Drone Army" Is Making Russia Sweat. *Forbes*. <https://www.forbes.com/sites/kellyaratherton/2022/09/01/ukraines-inexpensive-drone-army-is-making-russia-sweat/>

Balmforth, T., & Astakhova, O. (2022, March 16). Russian air force struggles for control of Ukraine's skies. *Reuters*.

BBC News. (2022, February 24). Russia attacks Ukraine: Moscow's assault enters third day. *BBC*. <https://www.bbc.com/news/world-europe-60506682>

Bendett, S. (2022, April 8). Russia's Robot Army Made Moves in Ukraine, *Too*. *Defenseone.com*. <https://www.defenseone.com/ideas/2022/04/russias-robot-army-made-moves-ukraine-too/362858/>

Bendett, S., & Leed, M. (2022). Russia's Weapons of the Ukraine War. *CNA Occasional Paper*.

Bendikaitė, D. (2023, February 24). Ukraine claims it has destroyed over 2,600 Russian tanks since start of war. *Newsweek*. <https://www.newsweek.com/ukraine-russia-tanks-destroyed-combat-vehicle-losses-1783967>

Ben-Israel, G. (2008). Databases on Terrorism: Constructing a Database on Hostage-barricade-terrorism and Abductions. In M. Kauffmann (Ed.), *Building and Using Datasets on Armed Conflicts* (pp. 63-73). Amsterdam, the Netherlands: IOS Press.

Ben-Israel, G., & Shorer-Zeltser, M. (2012). Telling a Story by Dry Statistics: Islamic Radical Suicide Terror Attacks in Israel (1993-2008). In T. Dronzina & R. E. Houdaigui (Eds.), *Contemporary Suicide Terrorism: Origins, Trends, Ways of Tackling* (pp. 52-67). Amsterdam, the Netherlands: IOS Press.

Ben-Israel, G. (2014). Development of Defense-Oriented Application Software under Fire: The Case of Israel. In A. Vaseashta, P. Susmann, & E. Berman (Eds.), *Cyber Security and Resiliency Policy Framework* (pp. 115-126). Amsterdam, the Netherlands: IOS Press.

Ben-Israel, G. M. (2018a). The Impact of Web 2.0 on Public Engagement in the Israeli Home Front from the 2006 Lebanon War to the 2014 Israel-Gaza Conflict. *International Journal of Public Administration in the Digital Age*, 5(2), 52-63.

Ben-Israel, G. M. (2018b). Telling a Story via Tumblr Analytics: Europe's Young Muslim Female Attraction to ISIS. *International Annals of Criminology*, 56(1-2), 55-78. <https://www.cambridge.org/core/journals/international-annals-of-criminology/article/telling-a-story-via-tumblr-analytics-europes-young-muslim-female-attraction-to-isis/FEA7F58A3960DD9F5A76346F8213F476>

Brumfield, B. (2023, June 15). Foreign funding of U.S. universities: A national security concern? *National Counterintelligence and Security Center*. <https://www.dni.gov/ncsc-features/2023-06-15-feature-story-foreign-funding-us-universities.html>

Carpenter, T. G. (2023, March 15). The Emerging Russia-China Axis: The Return of Bipolarity? *Cato Institute*. <https://www.cato.org/commentary/emerging-russia-china-axis-return-bipolarity>

Eilam, E. (2014). The Next War between Israel and Hamas: Learning from Operation Protective Edge. *Israel Journal of Foreign Affairs*, 8(3), 49-58. <https://doi.org/10.1080/23739770.2014.11446600>

Europol. (2024). *European Union Terrorism Situation and Trend Report 2024*. Publications Office of the European Union.

Federman, J., & Magdy, S. (2023, November 25). Qatar's role as mediator in Israel-Hamas war puts fraught relationships with both sides to the test. *Associated Press*. <https://apnews.com/article/israel-hamas-war-qatar-mediator-hostages-f6a6cf8431c595acea4cd1d90a1f80f6>

Flanagan, S. J., Kirchberger, S., & Kreuzer, M. P. (2022). Russia's Invasion of Ukraine in 2022. In M. P. Kreuzer (Ed.), *The Russo-Ukrainian War: Causes, Course, Consequences* (pp. 7–26). PRIF Reports No. 9. <https://www.hsfk.de/publikationen/publikationssuche/publikation/the-russo-ukrainian-war-causes-course-consequences>

Golovan, M. (May 3, 2024). *Liga.net*. <https://news.liga.net/en/politics/news/general-pavlyuk-drony-izmenili-geografiyu-i-taktiku-polya-boya-a-pehota-zasela-glubzhe>

Gross, J. A. (2023, October 11). Hamas filmed its massacres, and made sure the world would see them. *The Times of Israel*. <https://www.timesofisrael.com/hamas-filmed-its-massacres-and-made-sure-the-world-would-see-them/>

Gross, J. A. (2024, January 5). Inside Hamas's homegrown rocket arsenal, the weapon that started the war. *The Times of Israel*. <https://www.timesofisrael.com/inside-hamass-homegrown-rocket-arsenal-the-weapon-that-started-the-war/>

Harel, A., & Kubovich, Y. (2023, October 10). How Hamas Managed to Catch Israel Off Guard. *Haaretz*. <https://www.haaretz.com/israel-news/2023-10-10/ty-article/premium/how-hamas-managed-to-catch-israel-off-guard/0000018b-139d-d6e6-a9df-97bd13140000>

- Hecht, E. (2023, December 1). Hamas's Military Capabilities: Rockets, Drones, and More. *The Washington Institute for Near East Policy*. <https://www.washingtoninstitute.org/policy-analysis/hamass-military-capabilities-rockets-drones-and-more>
- Heller, A., & Lubell, M. (2023, October 8). Hamas surprise attack out of Gaza stuns Israel and leaves hundreds dead in fighting, retaliation. *Associated Press*. <https://apnews.com/article/israel-palestinians-gaza-hamas-rockets-airstrikes-tel-aviv-11fb98655c256d54ecb5329284fc37d2>
- Hoffman, F. G. (2009). Hybrid Warfare and Challenges. *JFQ*, 52, 1st quarter, 34-39. <http://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-52.pdf>
- Intelligence and Terrorism Information Center. (2023, November 2). *Iran's support for Hamas: Overview and assessment*. <https://www.terrorism-info.org.il/en/irans-support-for-hamas-overview-and-assessment/>
- Kagan, F. W., Barros, G., Stepanenko, K., & Clark, M. (2023). *Russian Offensive Campaign Assessment*. Institute for the Study of War. <https://www.understandingwar.org/backgrounders/russian-offensive-campaign-assessment-february-24-2023>
- Kaldor, M. (2012). *New & Old Wars: organized violence in a Global Era* (3rd Ed.). Stanford, California: Stanford University Press.
- Katz, Y. (2023, October 15). Exclusive: The October 7 Hamas battle plan. *The Jerusalem Post*. <https://www.jpost.com/arab-israeli-conflict/article-769911>
- Kingsley, P., & Kershner, I. (2023, October 7). Hamas Attacks Israel in Surprise Assault, Setting Off War. *The New York Times*. <https://www.nytimes.com/2023/10/07/world/middleeast/israel-gaza-hamas-attack.html>
- Kirby, P. (2022, February 24). Why has Russia invaded Ukraine and what does Putin want? *BBC News*. <https://www.bbc.com/news/world-europe-56720589>
- Kirby, P. (2022, April 30). Ukraine war: Why has Russia's invasion failed? *BBC News*. <https://www.bbc.com/news/world-europe-60946340>
- Kofman, M., Milley, P., & Waterlow, K. (2022, August 24). Why Did Putin Miscalculate in Invading Ukraine? *War On The Rocks*. <https://warontherocks.com/understanding-the-russo-ukrainian-war-a-guide-from-war-on-the-rocks/>
- Lisnyansky, D. (2024). *The evolution of pro-Palestinian activism in Europe post-October 7*. Middle East Institute Policy Paper.
- Marcus, I., & Shuster, H. (2023, December 15). *Hamas's combat tactics in Gaza: A comprehensive analysis*. Jerusalem Center for Public Affairs.
- UN Human Rights Office. (2023, November 30). *UN experts condemn atrocities by Hamas, call for immediate release of all hostages*. <https://www.ohchr.org/en/press-releases/2023/11/un-experts-condemn-atrocities-hamas-call-immediate-release-all-hostages>
- Rubin, U. (2011). *The Missile Threat from Gaza: From Nuisance to Strategic Threat*. Begin-Sadat Center for Strategic Studies. <https://besacenter.org/wp-content/uploads/2011/11/MSPS91.pdf>

Sabadus, L. (2022, April 7). Vladimir Putin: What was the Russian president's reasoning for invading Ukraine? *The Scotsman*. <https://www.scotsman.com/news/world/vladimir-putin-what-was-the-russian-presidents-reasoning-for-invading-ukraine-3638120>

Schanzer, J. (2018). *State of Play: Qatar's Funding of Hamas*. Foundation for Defense of Democracies. <https://www.fdd.org/analysis/2018/09/17/state-of-play-qatars-funding-of-hamas/>

Scales, R. H., & Ollivant, D. (August 1, 2014). "Terrorist armies fight smarter and deadlier than ever". *The Washington Post*. https://www.washingtonpost.com/opinions/terrorist-armies-are-fighting-smarter-and-deadlier-than-ever/2014/08/01/3998ae00-18db-11e4-9e3b-7f2f110c6265_story.html

*Batya Brutin*¹
**HOLOCAUST ICONS IN VISUAL ART AND
THE ISRAELI-PALESTINIAN CONFLICT**

Abstract

The Jewish-Arab conflict dates to the end of the nineteenth century and intensified because of the United Nations Resolution 181 in 1947, in which the British Mandate of Palestine was divided into Arab and Jewish states. The first Arab-Israeli war, 1948-1949, was ignited by the declaration of an independent State of Israel. As result of the war, the territory was divided into three parts: the State of Israel, the West Bank of the Jordan River, and the Gaza Strip. Over the following years, tensions escalated in the region, particularly between Israel and the countries surrounding it and the political-ideological Arab organizations. Icons of the Holocaust are a significant component of art and appear in different contexts, such as the Israeli-Palestinian conflict. The artists manifest the political context by utilizing the famous image of the little boy with his hands raised during the Warsaw Ghetto liquidation, the image of Anne Frank, and the image of the well-known phrase Arbeit Macht Frei on six concentration camps gates, especially the one in Auschwitz². The discussion will combine the artistic-biographic approach and socio-historical reference to create a link between the iconographic and stylistic artistic debate and the historical time and the social-cultural context in which the artworks were created. The connection between Holocaust icons and the Israeli-Palestinian conflict, which has not been done before, will present an analysis that will emphasize the visual expressions and interpretations used to express and convey the artists' political ideas and messages about the topic.

Keywords: *Holocaust, Israeli-Palestinian conflict, Anne Frank, the Warsaw Ghetto boy, Arbeit Macht Frei.*

This paper discusses the use of Holocaust icons in visual representations, mostly caricatures and street art, on the topic of the Israeli-Palestinian conflict. It examines how these icons are depicted, how they are used, and their meaning in connection to the Israeli-Palestinian conflict. The paper is an ongoing study that relies on my previous research and presents new materials that were not included in it (Brutin 2019; Brutin 2021).

¹ Beit Berl Academic College, Israel and WHISC (Women in the Holocaust - International Study Center), batyab@netvision.net.il

² *Arbeit Macht Frei* in German means *Work Sets You Free*.

The Jewish-Arab conflict backdates to the end of the nineteenth century and escalated because of the United Nations Resolution 181, known as the Partition Plan, in 1947, when the region was under the British Mandate of Palestine in the years 1920-1948. The United Nations plan was that the British Mandate of Palestine would be divided into two states, one Arab and one Jewish. The Arab leaders rejected the United Nations proposed plan, so the declaration of an independent State of Israel ignited the first Arab-Israeli war in 1948-1949. As result of the war, the territory was divided into three parts: the State of Israel, the West Bank of the Jordan River, and the Gaza Strip. During and after the war, hundreds of Arab villages were abandoned or destroyed in the territory of the State of Israel and hundreds of thousands of Arab residents were forced to leave their homes under various circumstances and became refugees. After the war, most of them were forbidden by the Israeli government to return to their homes and settled in the West Bank of the Jordan River and the Gaza Strip. Since then, the tension between Israel and Arabs escalated in the region, particularly between Israel and the countries surrounding it and the political-ideological Arab organizations (Herzog and Gazit, 2005; Kattan, 2009).

Icons of the Holocaust are a significant component of art referring to the Holocaust and appear in different contexts as well. Artists manifest their ideas and messages by utilizing the famous image of the little boy with his hands raised during the Warsaw Ghetto liquidation, the image of Anne Frank, and the image of the well-known phrase Arbeit Macht Frei on concentration camps gates, especially the one in Auschwitz I. We will discuss how artists have integrated images of the Holocaust into their artworks to address the Israeli-Palestinian conflict.

Many artists were influenced by well-known Holocaust photographs produced by Nazis, Jews, neutral and they rely on them in their artworks to convey their ideas and messages. Janina Struk wrote that In order to be able to interpret a photograph, there must be some knowledge of the event being photographed (Struk, 2004). Therefore, the artists relied on famous photographs in order to immediately attract the viewer's attention; sometimes they receive the spectator's acceptance and occasionally his rejection.

Since most of the examples in this paper are caricatures, it is important to explain that this form of art has been with us for hundreds of years. The caricaturists have a particular point of view serving a political purpose by rendering images in a simplified or exaggerated way; they present their ideas powerfully by using images, mainly well-known, to promote, analyze and criticize political issues. The purpose of the caricatures is to reflect on a given situation and provoke debate.

Street art is also presented in this paper. It is a visual art genre created and presented in public locations to be part of daily life as a reminder of an issue or a phenomenon. Street art evolved from the artistic form of graffiti. While graffiti is based on simple written words, street art presents images to convey messages and meanings.

This paper is in the field of art history; therefore, it focuses on the visual expressions of the topic. The discussions about them create a link between the iconographic and artistic debate and the historical time of creation to provide a social, cultural, and political contexts.

The questions I try to answer are: In what way have the artists used Holocaust icons to represent the Israeli-Palestinian conflict? What are the meanings and messages that the artists convey through these icons?

Before getting into the discussion about the appearance of Holocaust icons in visual presentations, one must understand that children are the first to be affected and used as a "weapon" during wars and political conflicts. The first Holocaust icon we will discuss is the famous image of the little boy with his hands raised during the Warsaw Ghetto liquidation. He first appeared in a photograph in the German General Jürgen Stroop's report to Adolf Hitler of 1943 (Figure 1) (Stroop, 1979).³ The boy appears in short pants, boots, coat, and cap, behind him there is a convoy of Jewish men, women, and children raising hands as well or carrying bags. Nazi soldiers are guarding them, while on the right one of them is pointing his submachine gun at the boy.

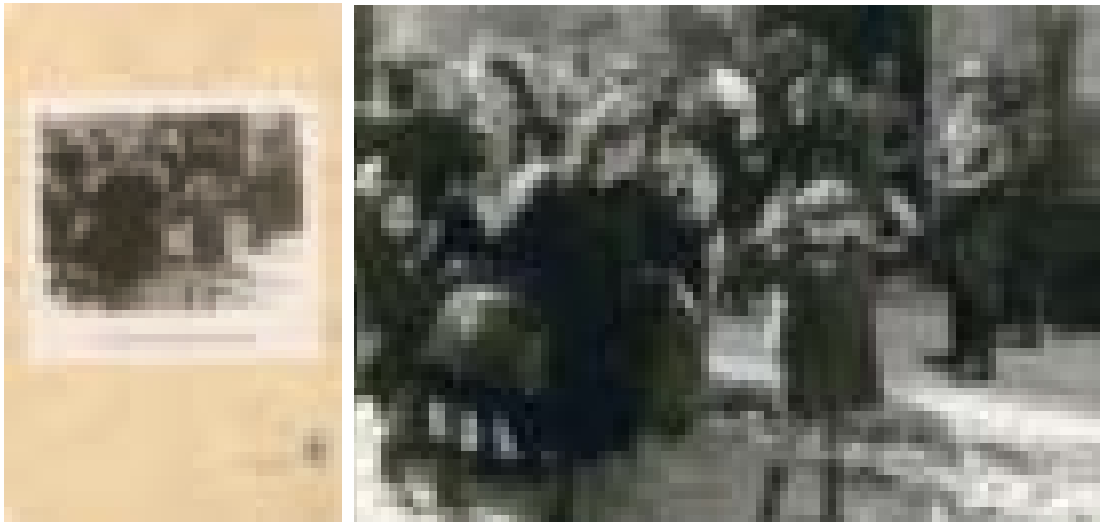


Figure 1. *Photograph from the Warsaw Ghetto. General Jürgen Stroop's report of 1943.*

Marianne Hirsch described the photograph in these words: "If you had to name one picture that signals and evokes the Holocaust in the contemporary cultural imagination, it

³ Jürgen Stroop was an SS officer, the commander of the fight against the Jewish uprising in Warsaw Ghetto in 1943. His mission was to eliminate the Warsaw Ghetto. Stroop prepared a decorated album for Adolf Hitler including reports on the battle in Warsaw and a series of photographs taken by the Germans during the Jewish Warsaw Uprising and the liquidation of the Warsaw Ghetto. On the front cover, the inscription, in beautiful German calligraphy, states "Es gibt keinen jüdischen Wohnbezirk in Warschau mehr!" (There is no longer the Jewish quarter of Warsaw).

might well be the picture of the little boy in the Warsaw ghetto with his hands raised. The pervasive role this photograph has come to play is indeed astounding: it is not an exaggeration to say that, assuming an archetypal role of Jewish (and universal) victimization, the boy in the Warsaw ghetto has become the poster-child for the Holocaust" (Hirsch, 2002).

Some of the artists used the entire original photograph from Warsaw. Other artists added a single Nazi soldier aiming his machine gun at the Warsaw boy. Most of the artists isolated the Warsaw boy's figure from the convoy in the photograph. All the artists portrayed the Warsaw boy with additional elements to express their point of view.

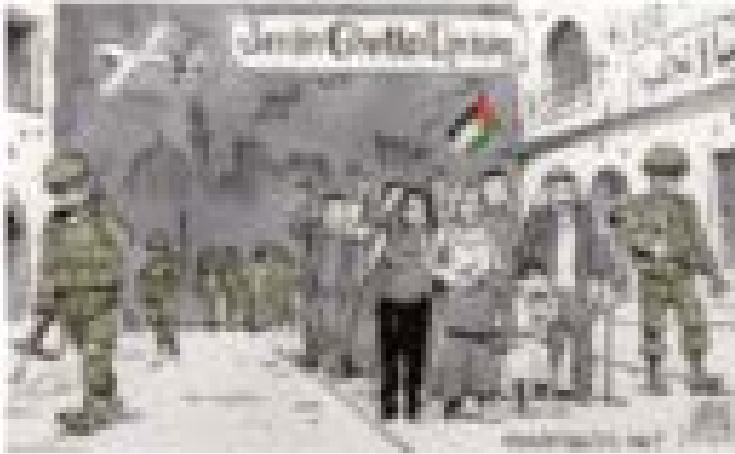


Figure 2. *Carlos Latuff, Jenin Ghetto Uprising, 2023.*

Brazilian political activist and cartoonist Carlos Latuff uses the iconic photograph with the little Jewish boy from the Warsaw Ghetto several times through which he conveys political and critical messages concerning the Israeli-Palestinian conflict. He considers himself as having "Arab roots" because he is a Brazilian of Lebanese ancestry. Latuff is best known for his caricatures depicting scenes connected to the Israeli-Palestinian conflict and the Arab Spring events on Indymedia, the Independent Media Center, websites, and private blogs. Sometimes he compares Israel's practices to Nazism to declare his objection and criticism about Israel's actions in Gaza (Brutin, 2019).

In *Jenin Ghetto Uprising* of 2023 (Figure 2) Latuff refers to the confrontation in the Jenin refugee camp in the Palestinian Authority that took place on January 26, 2023, between the Israel Defense Forces and the Palestinian terrorists. The Israeli authorities explained that the battle broke out following the Israeli security forces attempts to thwart a terrorist attack which was planned by the Palestinian Islamic Jihad and was already in the preparation stage. In this event, 11 Palestinians were killed, including 10 armed terrorists and one passerby. In addition, 20 others were injured, and a number of terrorists were arrested. Israeli forces dropped a leaflet to Palestinian residents to stay away from the area that the Israeli air force was about to attack. Thousands of Palestinian families were forced out of their homes to seek safety, while the Israeli forces tear-

gassed the families (Qasem, 2023). Mahmoud Abbas, the Palestinian president, condemned the event and called it a massacre (Sawafta, 2023).

In the cartoon (Figure 2) Latuff clearly meant to rely on the iconic Holocaust photograph from the Warsaw Ghetto liquidation. Instead of the Jewish group, the artist depicted a group of Palestinians, old men and one woman, a young woman wearing a *Palestinian Keffiyeh*⁴ and a little girl holding a stuffed toy. A few men and the young woman are raising their hands in surrender. The scene is depicted against the backdrop of a street in the refugee camp with a Palestinian flag waving on one of the buildings, and armed soldiers escorting the group of people. On the left there is unidentified airplane and on the right side a huge sign saying "Jenin Ghetto Uprising" referring to the armed resistance by the Palestinian Islamic Jihad fighters.

On October 7, 2023, a tragic event befell Israeli society. Hamas, the Arab terror organization, broke out the fence between the Gaza Strip and the Israeli civilian communities and brutally and cruelly murdered, raped, beheaded 1,400 innocent women, men, children, and babies, and looted and burnt their property. They kidnapped 240 inhabitants, among them 30 children.⁵ The Hamas attacked defenseless, noncombatant civilians just because they are Jewish. These events immediately evoke the memory of the greatest catastrophe in Jewish history – the Holocaust.

It is not the first time that Italian contemporary satirical artist and activist Alessandro Palombo uses both the Warsaw boy and Anne Frank's images to deal with the phenomenon of anti-Semitism. He did it before in the series of drawings *Never Again*, through mimicking characters from the long-running American sitcom animated television series *The Simpsons* created by Matt Groening for the Fox Broadcasting Company (Brutin, 2019; Brutin, 2021; Brutin, 2024). These two images appear again in his current murals street art in which he responds to the horrible events of October 7, and at the same time to the growing anti-Semitism with a message of hope to the world and future generations.

In his current murals' street art in New Gate, Milan (Porta Nuova, Milano) from the series *Innocence, Hate and Hope*, 2023 (Figure 3), Palombo portrayed the Warsaw Ghetto boy with his hands raised in one of his drawings. He added a yellow Star of David on the boy's coat to emphasize his Jewishness (Brutin, 2019).⁶ On both sides of the boy, as if trapping him, he depicted a single Hamas armed terrorist, on the right wearing a black head and face cover as well as a green band around his head. He is aiming his weapon at the boy, while on the left side he shows a Palestinian boy wearing Hamas uniform and a green band around his head. He is holding a machine gun pointing

⁴ The Palestinian Keffiyeh is a scarf characteristic of a fishnet-style black-and-white pattern. Since the beginning of the Israeli–Palestinian conflict, it has become a prominent symbol of Palestinian nationalism.

⁵ At the time this article is written, there are still 134 hostages in Gaza Strip.

⁶ The addition of the yellow Star of David is a factual-historical mistake, since in the Warsaw Ghetto the inmates wore white armbands with a blue Star of David.

towards the boy with determination. This Palestinian Hamas boy represents the Hamas ideology of killing the Jews, which he was educated from childhood. This is the "face" of the next generation of Hamas. Palombo stated, "The anti-Semitic rage unleashed by Hamas is flooding the Jews in all parts of the world. This horror that returns from the past must make us all ponder because it undermines the freedom, security, and future of each one of us. Terrorism is the very denial of humanity and has nothing to do with resistance, it uses us to divide and drag us into its abyss of evil, into an infernal vortex that finds no end. There cannot be peace until these mistakes are erased, since legitimizing it means condemning all humanity to death" (Russo, 2023).



Figure 3. aleXsandro Palombo, *Innocence, Hate and Hope*, 2023, Porta Nuova, Milan, Italy.

The artist conveys his moral message through a child of the Jewish past of the Holocaust, while showing a child on the Hamas aggressor's side of the present, without mentioning the current innocent, harmless Jewish Israeli children, victims of the inhuman terror attack by Hamas on October 7.

Palombo's current mural street art is an important message of warning to the world in general and to the Palestinian people in particular, to change their aggressive, anti-Semitic actions towards Jewish population in the name of Islamic ethics, and instead, to invest in educating the young generation of antiwar, peace, humanistic values. By using this icon, the artist succeeds to immediately capture the spectator's full attention to his messages.

Israeli ultra-orthodox caricaturist Avishai Chen also referred to the horrific event of October 7 (Figure 4).



Figure 4. Avishai Chen, October 7 - *"We have no one to lean on but our Father in Heaven"*, 2023, Israel.

Against the background of high clouds in dark brown tones that look like a screen, the artist depicts a quiet community with beautiful houses with red roofs and greenery around them. Between the houses, on both sides, the Israeli flags are waving. In the center of the depiction, on cracked green ground and a heavy shadow, a tall Hamas soldier can be seen wearing a belt of bullets while pointing his weapon at a boy who raises his hands in surrender, wearing a cloak with an Israeli flag on it to identify him as Israeli. He is wearing sports clothes, shorts, gym shoes and a shirt with the date 2023 on it. The figure of the boy is undoubtedly reminiscent of the boy from Warsaw and the Hamas soldier the Nazi soldier pointing his weapon at him. As then, even now the Jewish child is not protected from his enemies who want to murder him (Levin, 2023).

The second Holocaust icon is the image of Anne Frank from the photographs she added to her diary written while being in hiding from the Nazis (Figure 5).



Figure 5. Anne Frank in Amsterdam, 1942. Photograph taken by her father Otto Frank.

Anne, Annelies Marie, Frank was born in Frankfurt am Main, Germany, on June 12, 1929. In 1934, after the Nazis had risen to power in 1933, she fled with her family to Amsterdam, Holland. In July 1942 the family went into hiding from the Nazis, in a Secret Annex of the building where her father, Otto Frank, worked. On August 4, 1944, the Gestapo caught her and her family and sent them to Westerbork, a Nazi transit camp in The Netherlands. From there she was sent to Auschwitz concentration camp in Poland, and finally to Bergen Belsen, the concentration camp in Germany where she died at the age of sixteen.

Anne Frank became famous because of her diary and her photographs which are internationally known. Anne Frank's "face" has been adopted by many artists mostly as a source of inspiration to express their feelings and ideas about the Holocaust as well as to express their political opinion on Israeli-Palestinian conflict. She, like the Warsaw boy, became an icon of the Holocaust in general and as a representative of the innocent and vulnerable Jewish children during the Holocaust.



Figure 6. Unknown Artist, *Anne Frank Wearing a Palestinian Keffiyeh*, 2007, behind the Central Station, Amsterdam



Figure 7. Unknown Artist, *Anne Frank Wearing a Palestinian Keffiyeh*, 2018, Witwatersrand University, Johannesburg, South Africa.

Numerous street art works from the 2000s portrayed Anne Frank wearing a Palestinian Keffiyeh, most of which rely on the photograph taken by her father Otto Frank in 1942 which she attached to her diary (Figure 5). This depiction seems to be a popular street art in different cities around the world, such as Amsterdam, New York, and other places, especially as a reaction to the Israeli attacks on Palestinian targets (Figures 6, 7). The depiction from Witwatersrand University, Johannesburg, South Africa (Figure 7) was created by students of the Palestinian Solidarity Committee as a flyer for the annual Israel Apartheid Week at the University. They portrayed Anne Frank wearing a Palestinian Keffiyeh to draw attention to the Palestinian situation as they see it. A student who took part in poster design tweeted: "This is a flyer that draws attention to the fact that the same racism, hardship, and oppression that was faced by Jews during the Nazi times is now being directed towards Palestinians". The South African Union of Jewish Students expressed strong reservation to the use of a symbolic Jewish Holocaust victim to promote a blatantly anti-Semitic agenda (Cohen, 2018).



Figure 8. aleXsandro Palombo, *Two Girls, Innocence, Hate and Hope*, 2023, Porta Nuova, Milan, Italy.

In another drawing in the series *Innocence, Hate and Hope*, aleXsandro Palombo shows two girls (Figure 8); one is Anne Frank with a striped camp prisoner uniform lamenting over the harsh events during the Holocaust in the past when the Jewish people had no state, as well as over the horrific events on October 7 in the State of Israel, represented by its flag. The other girl is a Palestinian girl with a Keffiyeh, and the Palestinian flag tied to her head; she wants to free Gaza Strip, as written on her face, from the Hamas, the cruel, merciless Arab terror organization. Her almost impossible rebellion is symbolically shown by the slowly burning Hamas flag for a better future of the next generations. Palombo wants to teach the children in Gaza Strip mercy and peace to achieve hope and peaceful life (Russo, 2023).⁷

⁷ The author's correspondence and telephone interview with Vanessa Esteban, assistant to Palombo aleXsandro, November 2023. On November 29, 2023, this street painting was brutally damaged as an anti-Semitic action.

The third Holocaust icon that artists used to deal with the Israeli-Palestinian conflict is the well-known phrase *Arbeit Macht Frei* on six Nazi concentration camps entrance gates, especially the Auschwitz I gate (Diefenbach, 1873; Cywiński, Lachendro and Setkiewicz, 2013; Greif and Siebers, 2016).⁸

Against the background of the *Gaza war*, December 27, 2008-January 18, 2009, known as *Operation Cast Lead* on the Israeli side and *Gaza Massacre* on the Arab side, the Arab press published cartoons with anti-Semitic motifs, including those containing motifs from the Nazi extermination camps, such as the famous phrase *Arbeit Macht Frei*. For example, a caricature made by Imad Hajjaj in the Jordanian *Al-Ghad* on January 4, 2009 (Figure 9) (MEMRI, 2009).⁹

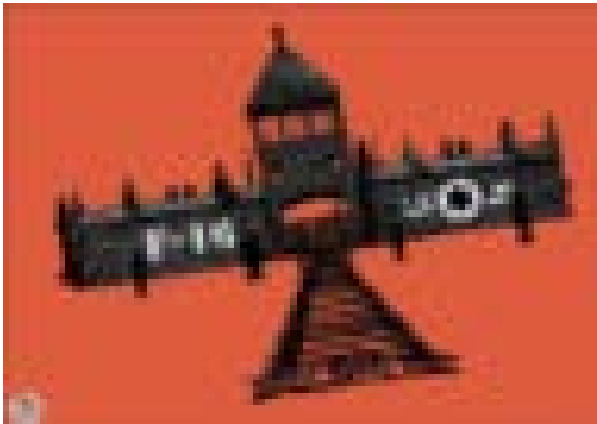


Figure 9. Imad Hajjaj, *Arbeit Macht Frei*, January 4, 2009, *Al-Ghad*, Jordan.

On a red backdrop the artist portrayed an Israeli F16 aircraft as a model of the Auschwitz-Birkenau notorious extermination camp, and on the tail of the aircraft he added the inscription *Arbeit Macht Frei*. He shows the now strong Israel attacking the vulnerable people of Gaza behaving as the Nazis, forgetting the Nazi actions towards

⁸ The *Arbeit Macht Frei* inscription originates from a German novel's title written by the German philologist and novelist Lorenz Diefenbach (1806–1883), in 1873. The meaning of the slogan in the novel was to describe the process of "repentance" gamblers and crooks went through productive work to adopt moral norms of honesty. The Weimar Republic adopted this slogan to expedite the proactive work policy to reduce the level of unemployment in post-World War I Germany. When the Nazis rose to power in 1933, they continued to use the slogan in its original meaning for the same reason, so when the Nazis established concentration camps for dissidents in Germany, it was only natural for them to inscribe *Arbeit Macht Frei* on the camp gates, but this time they used it as a deception and irony to instill false hopes in the prisoners' minds to prevent insurrection. Theodor Eicke (1892–1943), commander of Dachau concentration camp, was the first to install words *Arbeit Macht Frei* on the Dachau concentration camp gate, and other camps soon followed: Sachsenhausen, Flossenbürg, and Groß-Rosen. When established the Theresienstadt Ghetto/Camp, the Nazis placed the inscription on the Small Fortress there. Following the occupation of Poland and the establishment of the Auschwitz I camp, the Nazis positioned on top of the camp entrance gate the false and deceitful slogan *Arbeit Macht Frei*.

⁹ <https://www.jewishvirtuallibrary.org/gaza-war-anti-semitic-cartoons>; <https://hajjajcartoons.com/ArchiveBy-Month?month=January&year=2009> (accessed on January 27, 2024).

the harmless, haunted, and helpless Jewish people in the Auschwitz-Birkenau death camp. By adding the words *Arbeit Macht Frei* he combines Auschwitz I, where the sign *Arbeit Macht Frei* hanged on the entrance gate, and the Auschwitz-Birkenau death camp, where millions of Jews were murdered, to intensify the scene, to draw attention to what is happening in Gaza, and to emphasize that Israel is worse than the Nazis.



Figure 10. Vasco Gargal,
Crematorium, 2020, Portugal.

In his caricature *Crematorium* (Figure 10), Portuguese cartoonist Vasco Gargalo showed Israeli Prime Minister Benjamin Netanyahu wearing a black suit and a black *Skullcap*¹⁰ and a blue armband with a *Shield of David*¹¹ in a white circle on it, reminiscent of the armband Jews were forced to wear in several ghettos during the Holocaust (MPPM, 2020; MEMRI, 2023). The artist chose the blue and white colors, as the colors of the flag of Israel, to emphasize Netanyahu's national identity. His facial features are grotesque, large ears, and long nose, reminiscent of the Nazi anti-Semitic caricatures. He is pushing a coffin, wrapped with the Palestinian flag, into a crematorium at Auschwitz. To specify the place, the artist added the well-known words *Arbeit Macht Frei*, although the mass murdering of the Jewish people occurred in Auschwitz-Birkenau and the sign was at Auschwitz I. This historical mistake did not prevent the artist from using this slogan, since it is more known. The message the artist conveys here is that Israel, under the ruling of Netanyahu, is burning the Palestinian dead victims, represented by their flag. By combining the Nazi sign *Arbeit Macht Frei* and the crematorium, Gargalo states that the Israeli do exactly what the Nazis did to the Jewish victims' bodies in the concentration camps. This is a wrong historical comparison that serves the Palestinian ideology and its supporters.

Even though Gargalo was aware of the strong reaction to this depiction, he stressed that "It is my view on this attack. When I did the cartoon, I knew it was strong, that I was going to touch on the issue of the victims of Holocaust, but in fact I do not add anything to what I see. It's a comparison I made of the Israeli-Palestinian conflict" (Irancartoon, 2019).

¹⁰ *Skullcap* is a Kippa in Hebrew.

¹¹ Star or Shield of David is Magen David in Hebrew.

CONCLUSION

This paper provides the readers with the insight of artistic representations of the Israeli-Palestinian conflict. Artists described it each in their own artistic style and from their political point of view. All of them relied on photographs of icons of the Holocaust, the little boy with his hands raised during the Warsaw Ghetto liquidation, the image of Anne Frank, and the image of the well-known phrase *Arbeit Macht Frei*, to convey ideas, meanings, and messages about the Israeli-Palestinian conflict. The use of the well-known images immediately evokes the spectator's attention to the depiction and he either agrees and sympathizes, or he rejects and protests against what is portrayed.

The Israeli-Palestinian conflict is still unfolding and certainly there will be more artistic responses in the recent future. Will the artists continue to use icons that represent the Holocaust? Only time will tell.

RERERENCE LIST

Brutin, B. (2019). *Holocaust Icons in Art: The Warsaw Ghetto Boy and Anne Frank*. Jerusalem: The Hebrew University Magnes Press and Berlin, Berlin: De Gruyter.

Brutin, B. (2021). *Etched in Flesh and Soul: the Auschwitz Number in Art*. Berlin: De Gruyter.

Brutin, B. (2024). *'Arbeit Macht Frei': Representations and Meanings in Art*. Berlin: De Gruyter.

Cohen, H. (2018, March 19). *South African Students Create Palestinian Anne Frank for Israel Apartheid Week*. Retrieved February 27, 2024, from <https://forward.com/fast-forward/396835/south-african-students-create-palestinian-anne-frank-for-israel-apartheid/>

Cywiński, P. M. A. Lachendro J. & Setkiewicz, P. (2013). *Auschwitz from A to Z, an Illustrated History*. Oświęcim: Auschwitz-Birkenau State Museum.

Diefenbach, L. (1873). *Arbeit Macht Frei – Erzählung* (Work sets you free – a story). Bremen: J. Kühnmann's Buchhandlung.

Greif, G. & Siebers, P. (2016). *Death Factory Auschwitz*. Cologne: Emons Verlag GmbH.

Herzog, C. and Gazit, S. (2005). *The Arab-Israeli Wars: War and Peace in the Middle East from the 1948 War of Independence to the Present*. New York: Vintage Books.

Hirsch, M. (2002). Nazi Photographs in Post-Holocaust Art: Gender as an Idiom of Memorialization. In O. Bartov & M. Nolan (Ed.), *Crimes of War: Guilt and Denial in the Twentieth Century*, (pp. 100–120). NY: New Press.

Iran cartoon. (2020, no date). *Cartoonist Vasco Gargalo targeted by threats and criticism for cartoon about Israel*. Retrieved January 27, 2024, from <https://www.iran-cartoon.com/site/news/cartoonist-vasco-gargalo-targeted-by-threats>

Kattan, V. (2009) *From Coexistence to Conquest, International Law and the Origins of the Arab-Israeli Conflict, 1891–1949*. London, New York: Pluto Press.

Levin, H. (2023, October 18). *Current cartoon gallery: “We have no one to lean on.”* Retrieved October 20, 2023, from <https://www.kore.co.il/viewArticle/142545> (Hebrew)

MEMRI. (2009, January 2). *Declaraciones antisemitas y caricaturas como consecuencia de la guerra en Gaza*. Retrieved January 27, 2024, from <https://www2.memri.org/espanol/declaraciones-antisemitas-y-caricaturas-como-consecuencia-de-la-guerra-en-gaza/2886>

MEMRI. (2023, October 27). *Qatari Media Compare Israel To Nazis, Netanyahu To Hitler; Gaza To Auschwitz*. Retrieved January 27, 2024, from <https://www.memri.org/reports/qatari-media-compare-israel-nazis-netanyahu-hitler-gaza-auschwitz>

MPPM. (2020, February 5). *Cartoonist Vasco Gargalo accused of “anti-Semitism”, targeted for censorship*. Retrieved January 27, 2024, from <https://mppm-palestina.org/content/cartoonist-vasco-gargalo-accused-anti-semitism-targeted-censorship>

Qasem, M. (2023, July 4). *Israel launches operation “Home & Garden” carrying the ongoing Nakba on the Palestinians*. Retrieved August 6, 2023 from <https://medium.com/@qasem3199/israel-launches-operation-home-garden-carrying-the-ongoing-f29a915f4872>

Russo, V. (2023, November 9). *Milano, nuovo murale di Alex Sandro Palombo: Anna Frank piange insieme a una bimba palestinese*. Retrieved November 13, 2023, from <https://tg.la7.it/cultura-e-societa/milano-nuovo-murale-di-alex-sandro-palombo-anna-frank-piange-insieme-a-una-bimba-palestinese-09-11-2023-198289>

Sawafta, A. (2023, October 13). *Palestinian President Abbas condemns violence against civilians*. Retrieved October 16, 2023, from <https://www.reuters.com/world/middle-east/palestinian-president-says-he-rejects-killing-civilians-both-sides-conflict-2023-10-12/>

Stroop, J. (1979). *The Stroop Report: The Jewish Quarter of Warsaw Is No More!*. New York: Pantheon Books.

Struk, J. (2004). *Photographing the Holocaust, Interpretation of the Evidence*. London-New York: I. B. Tauris.

*Sanja Đurđević*¹

GLOBAL RISE OF VIOLENCE AND NARCISSISTIC CULTURE - WHERE IS THE WORLD HEADING?

Abstract

We live in a postmodern society in which self-representation is more important than authentic human representation, in which it is difficult to determine which human needs are real, spontaneous and authentic needs, and which are imposed, useless to man but useful to large corporations. And although Christopher Lasch wrote about the culture of narcissism back in the 90s, his comments about modernity, which offers a fundamentally disturbed personality as its paradigmatic figure, are especially relevant today. Instead of real autonomy, people are subject to consumerism, overwhelmed by narcissistic self-affirmation, without guilt, in constant rivalry with others, with an unconscious unbridled urge to destroy those who stand in their way, immersed in the virtual world as a form of escape from the boring imperfect world. And if narcissism is essentially a defense against aggressive impulses, this explosion of narcissism inevitably produces individuals with borderline psychopathology who, through aggressive unscrupulous behavior, come to positions of power in the state, economy or criminal organization alike. In this paper, we are looking for answers to the questions of what are the consequences of living in such a society and with which concepts to understand phenomena such as the increase in violence, the increase in the number of suicides, the expansion of addiction to drugs, alcohol and medicines, the rise of fundamentalism and radical extremism. How capable are we to adequately respond to issues of human security in this world?

Keywords: *narcissism, aggression, violence, self-esteem.*

INTRODUCTION

When we are bombarded daily with images from the media about youth violence, family murders, unscrupulous corruption, hate speech, when friends let us down, when there are people who behave selfishly and exploitatively in the work environment, in politics, in the media, all of us, whether we are mental health experts or not, very often ask questions about the consequences of living in such a society and with which concepts to understand phenomena such as the increase in violence, the expansion of addiction to drugs, alcohol and medicines, the rise of fundamentalism, the rise number of suicides. Are we able to adequately answer the questions of human security, how to understand this

¹ Academy for Human Development, Belgrade, Serbia, djurdjevic.sanja26@gmail.com

much human injustice and what will happen next with our fragile planet? How will we protect mental health, if we know that the brain is a social organ, health is affected by numerous social circumstances? Our society definitely needs a significant shift towards a more humane world, but we wonder if people's mental health needs are in line with the wishes of capitalist societies (Djurđjević et al., 2022). As humans, do we stand a chance?

It is already commonplace that modern society is characterized by a lack of authenticity and originality and that this lack is manifested in the predominance of the false over the "real" self. The well-known 20th century social critic Christopher Lasch in his book *The Culture of Narcissism* (Lasch, 1980) wrote about the rise of modernity, which values appearance more than authenticity, offering a superficial, different and fundamentally disturbed personality as its paradigmatic figure. As Lasch says, the modern man is a new narcissist who is haunted not by guilt but by anxiety, who has lost loyalty to the group and considers everyone a rival. In the constant struggle for recognition in conditions of fierce competition, even when people manifestly accept competition, teamwork and cooperation, they actually unconsciously see in the competition an unbridled urge to destroy, at the same time harboring antisocial impulses in themselves (Đurđević, 2023). In a culture of competitive individualism, everyone is a potential enemy or at least a threat to everyone, and the pursuit of personal happiness reaches the limits of narcissistic self-absorption.

Is narcissism becoming simply a metaphor for the human condition today? It is difficult to provide precise data on the epidemiology of narcissistic personality disorder, but the literature most often mentions a range from 1 to 17% in the clinical population, or from 0 to 5.3% (0-6.2% according to DSM-5) in the general population. Findings from a large number of clinical and non-clinical studies suggest that narcissism is highly relevant in understanding aggression and violence. Research also shows that covert narcissism correlates to a greater extent with aggression compared to overt narcissism (Lambe et al., 2018; Zhang & Zhu, 2021).

The aim of this paper is to present scientific views on the phenomena of aggression and narcissism and their relationship from the perspective of the contemporary social context, because we believe that society and culture play a moderating role in the relationship between narcissism and aggression.

Society as a moderator of narcissism and aggression

Theorists from various scientific disciplines have constantly devised and revised theories about the mechanisms underlying aggression and violence. Early psychological theories focused on simple linear inferences about the causal mechanisms of aggression (eg Freud's theory of catharsis or the later theory of frustration). The shortcoming of these explanations of aggression is the neglect of many other potential causes of aggression, such as genetics, consciousness, cognition, affect, motivation, social environ-

ment. Newer theories and studies that support them do not deny that aggression is instinctive in nature, but claim that its manifestation in behavior is largely mediated by cognition and the environment (Bartholow, Sestir & Davis, 2005; Dodge, 2006).

Aggression is a normal part of the human character and the majority of individuals live peaceful lives without exhibiting extreme aggression or violence. But some individuals are characterized by strong aggressive impulses and their lives are filled with violence. Therefore, some people, thanks to the mechanisms of their cognitive resources, are able to reduce or eliminate the effects of aggressive impulses on their behavior, while in others these mechanisms seem to contribute to the exact opposite - that aggressive tendencies become stronger. According to Edwin H. Sutherland's theory of differential association, violent behavior is learned by a person through interaction with others, who allow or even encourage such behavior (Sutherland, 1972). Another explanation for instrumental aggression can be found in social learning theory (Bandura, 1977), according to which people learn their beliefs, behaviors, and aspirations from the social environment. Studies prove that individuals who grow up in a more violent environment tend to see the world as a hostile place, and violence as a method to resolve conflicts (Sestir & Bartholow, 2007).

Research has also shown that certain pro-aggression attitudes, values and beliefs can predict the level of general aggression (Huesmann & Guerra, 1997) as well as aggression towards certain groups of individuals (Malamuth et al., 1995) and aggression as a means of achieving social status (Rodkin et al., 2006). Also, there is a large number of studies that have proven the connection of aggressiveness with a hedonistic lifestyle. At the core of the concept of hedonism lies the human tendency to maximize pleasure and minimize dissatisfaction (Reiss, 2004). One of the values that characterizes modern culture is the hedonistic lifestyle, the need for enjoyment based on the "here and now" principle, the absence of a serious life plan, the unwillingness to sacrifice and postpone pleasure, the need for quick and easy enrichment. Or as Lasch described it as "living for the moment is the prevailing passion - living for oneself, not for one's predecessors or descendants" (Lasch, 1980: 5). An unbridled lifestyle has been used as a variable in numerous studies of the criminal population. Research in our community has shown that hedonism, contained in amorality, lies at the basis of criminal behavior, as well as that it successfully differentiates psychopathic from non-psychopathic criminals (Knežević, 2003; Kujačić, Međedović & Knežević, 2015; Radulović, 2006). Furthermore, the research of Đurđević et al. (2016) on a sample of the criminal population showed a substantial correlation between the variable of aggressiveness and the variable of hedonism. In this research, the result was that in both samples - general and criminal population, the second highly preferred value next to hedonism was materialism. But the difference between the samples was in the significance of the correlation of these two values. Namely, in the group of criminals, a significant positive correlation with

hedonism was found (in other words, with the increase in hedonism, the need to acquire material wealth also increased), while in the group of respondents from the general population, this correlation was not significant. Obviously, hedonism and materialism as two lifestyles can be seen as part of a broader value or life principle that material wealth should be acquired at any cost in order to be able to enjoy life and spend on everyday pleasures (Đurđević et al., 2016). The study by Kajonius and colleagues conducted on a sample of 385 Swedes and Americans, which aimed to determine the connection between the "dark triad" traits: Machiavellianism, narcissism and psychopathy and 10 universal social values, shows similar results. The results indicate the existence of a positive connection between hedonism and psychopathy, while Machiavellianism and narcissism positively correlate with the values of success and power (Kajonius et al., 2015).

We have witnessed that in today's society individual narcissism and the principle of achieving power "here and now" without excessive effort are highly supported, so it is not surprising that there are individuals who achieve these goals in an amoral way, through aggression and violence and/or interpersonal manipulation. Research provides evidence that precisely narcissism, psychopathy and especially Machiavellianism (three traits known in the literature as the "dark triad of personality") are very sensitive to the social context (Paulhus & Williams, 2002; Czibor & Bereczkei, 2012). Otherwise, individuals who have highly expressed these three traits are recognized by their expressed selfishness, manipulation, untrustworthiness, cold-blooded harming of others, need to control others. Often these people are characterized by disobeying social norms, which leads to social transgressions in terms of lying, cheating, manipulating, and stealing. Unfortunately, we witness that individuals with dark triad traits are often positively validated by society. One of the reasons for this lies in the fact that these individuals, even if they primarily try to find circumstances in which there will be a possibility to gain something for themselves, can at the same time be loyal friends, effective leaders and heroic rescuers (e.g. Hart, Richardson & Tortoriello, 2018; Patton, Smith & Lilienfeld, 2018; Smith et al., 2018). We will mention interesting research that links the characteristics of the dark triad and political leadership. Blais and Pruisers (2017) thus found that individuals with high prevalence of grandiose narcissism and Machiavellianism have a higher chance of winning political elections than others (Blais and Pruisers, 2017). These statements are supported by evidence from the study of Lilienfeld et al. (2012) that American presidents have higher levels of psychopathy than the normative sample of citizens (Lilienfeld et al., 2012). Also, related studies by Watts and colleagues (2013) show that American presidents have higher levels of grandiose narcissism compared to the normative sample (Watts et al., 2013). So how is it possible that voters do not recognize these traits? In addition to the explanation given by the congruence model of political preference, which emphasizes the mutual congruence of the characteristics and values of voters and leaders (Caprara & Zimbardo, 2004), according to some theorists, politicians not only hide these

dark characteristics of theirs from the citizens, but instead, through the political campaign, emit completely opposite characteristics, such as pleasantness, morality and humility (Campbell, 2016; Caprara et al., 2003). This is understandable if you know that narcissism, psychopathy and Machiavellianism have some unique characteristics in addition to their toxic core. Machiavellianism, for example, is characterized by a flexible, almost chameleon-like ability to use the strategy "from escape to cooperation" - in the sense of choosing behavior in relation to the situation, with the ultimate goal of gaining benefits for oneself, even at the cost of exploiting others. One study also showed that Machiavellianism is a significant positive predictor of fluid intelligence (Kowalski et al., 2018).

Narcissism, on the other hand, is also characterized by high vanity and grandiosity. Narcissistic people have a distorted self-assessment, that is, they believe that they are superior in their abilities compared to other people, and if this belief is rarely based in reality.

Psychopathy, as a third characteristic, includes impulsivity, recklessness, need for dominance and very low empathy towards other people. People who have a highly expressed dimension of this personality are by nature less flexible and more opportunistic in their behavior compared to people with a highly expressed dimension of Machiavellianism. Today, the term psychopathy has been replaced by the term borderline personality disorder (although the old term psychopathy can still be found in penological literature).

Certainly all three traits of the dark triad almost always involve dysfunctional interpersonal relationships, which are the result of selfish behavior and a lack of concern for others. These traits are more often investigated in clinical samples, in psychiatric or forensic institutions. In the literature on personality, these personality characteristics are referred to as normal personality dimensions, expressed as high or low (Divac, Jovanović & Švrakić, 2016). In clinical research, the presence of so-called pathological personality traits is used to derive one of the possible diagnoses of personality disorders; specifically, these personality traits are characteristic of cluster B disorders in the current diagnostic classification (DSM-5), which includes antisocial (socially irresponsible); borderline (emotional dysregulation); histrionic (attention-seeking) and narcissistic (poorly regulated and fragile self-esteem with exaggerated grandiosity) disorders. Recent genetic, neurobiological, and diagnostic studies suggest that impulsive aggression is one of the core dimensions of borderline personality disorder (Goodman & New, 2000). Research has estimated that the prevalence of borderline personality disorder is around 1.6% in the general population, while in the clinical population this percentage ranges up to 20% (Ellison et al., 2018). It is known that borderline pathology is characterized by unstable interpersonal relationships as well as frequent mistakes in reality testing, which causes difficulties in the personal, family and social functioning of these individuals. In the clinical context, to establish a diagnosis of borderline personality disorder, the presence of pathological, or extreme expression of at least 4 of the following 7 present characteristics is necessary: Emotional instability; Anxiety; Insecurity due to separation; Depressiveness;

Impulsivity; Exposure to risk; Hostility (outbursts of anger). It is impulsive, aggressive behaviors that include physical aggression directed at others, domestic violence, substance abuse, and property destruction that account for a significant portion of the morbidity and mortality associated with borderline personality disorder. Of course, since personality traits are formed through the two-way interaction of biogenetic dispositions and environmental factors, we cannot interpret the symptoms of the disorder outside of the context, that is, of the personality-environment interaction. Therefore, it can be reasoned that the development of borderline as well as narcissistic personality disorder can be greatly influenced by a social environment that supports and encourages violent behavior. Certain authors who dealt with the connection between rapid social changes and the increase in the level of psychopathology in the modern world assume that borderline pathology arises in the presence of a breakdown of community norms and values.

As for narcissism, it is certainly not a new phenomenon, so the claims that we live in the age of narcissism are called by some authors "putting old wine in new bottles" (Fine, 1986: 2). The fact is that the concept of narcissism has become a "hot topic" in numerous contemporary psychological theories. If we look at narcissism throughout the history of human civilization, we can say that it has long been reserved for a positive, acceptable description of the ruler as someone who is a grandiose, powerful superman to whom conventional norms do not apply, while when it appeared in "ordinary people", it was considered madness and eccentricity. In the later, renaissance age, in which the concept of individualization appears, we again have powerful individuals filled with unbridled individualism (or narcissism as we would describe it today) who often committed the most terrible forms of violence against others. So it can be said that today the interest is actually just slightly more shifted to the narcissism of the ordinary, average person. Otherwise, interest in narcissism has recently moved from the field of personality psychology (narcissism as a trait), clinical psychology and psychiatry (narcissistic functioning in personality disorders) to the field of organizational psychology, criminology, and political science.

Christopher Lasch in the aforementioned book *The Culture of Narcissism* talks about the fact that the narcissistic personality type is almost the prototype of modern society, that less extreme forms of narcissism are present to a large extent in people's everyday lives. As examples of these assertions, he cites some characteristic patterns of functioning such as: feeling of inner emptiness, ambivalence towards emotional attachment, suppression of anger, pseudo insights, calculated seductiveness, intense fear of old age and death, altered sense of time, fascination with celebrities, fear of competition, declining team spirit, deterioration of relations between men and women. A recent study examining the role of CEO personality traits on the relationship between entrepreneurial behavior and firm performance found that narcissism and Machiavellianism were particularly prominent personality traits of CEOs (Shirokova et al., 2024). Some studies that have investigated differences in the presence of narcissism in different cultures have found

that narcissism is positively correlated with individualistic traits and negatively correlated with collectivistic traits (Campbell, Rudich, & Sedikides, 2002). Both Heine and Hamamura (2007) found in their meta-analysis that individuals from Western individualistic cultures (especially the United States) have higher levels of extraversion and self-esteem - characteristics that are positively correlated with narcissism (Heine & Hamamura, 2007).

Before proceeding further, it is important to clarify the terms narcissism and self-esteem. According to Campbell and Miller, narcissism is a stable individual difference variable that can be reliably measured in normal (non-clinical) samples. Key components of the narcissistic personality include haughtiness, arrogance, the attitude of always being entitled to something (and asking others to agree to it), exploitative behavior (selfishly exploiting others in order to achieve one's own goals), self-sufficiency (preoccupation with fantasies of boundless success, power, beauty or ideal love), superiority (the belief that they are special) and vanity (Campbell & Miller, 2011). Self-esteem is most often conceptualized as a global, one-dimensional, affective evaluation of the self that can range from strongly negative to strongly positive.

Narcissism can be viewed from three aspects. The first aspect is how the narcissistic individual sees himself. This "self-view" is characterized by a feeling of uniqueness and specialness in relation to others. Another aspect is interpersonal relationships. A narcissistic individual uses others to fulfill his goals, resulting in superficial relationships without empathy, with a lot of manipulation. The third aspect is the strategies used by the narcissistic person to maintain their grandiose ideas about themselves. These strategies include seeking attention and praise, avoiding criticism. When these strategies are unsuccessful, narcissistic individuals may respond with aggression (Campbell & Miller, 2011). The connection between narcissism and physical aggression is accepted in the scientific literature, but there are differences among authors regarding the interpretation of the relationship between narcissism and aggression (Bettencourt et al., 2006; Bushman & Anderson, 1998). When talking about narcissism in the literature, one of the existing ways of describing a narcissistic individual is that he is a person who has a grandiose sense of himself as a mask to hide his low self-esteem (Zeigler-Hill & Besser, 2013; Baumeister et al., 2000; Cale & Lilienfeld, 2006).

The relationship between self-esteem and aggression is quite difficult to clarify and there is conflicting evidence in the scientific literature as to whether low or high self-esteem leads to aggression more easily. According to one view, low self-esteem leads to violent behavior, or at least there is a positive association between low self-esteem and high aggression (eg, Donnellan et al., 2005; Teng, Liu & Guo, 2015; Walker & Bright, 2009). Another view suggests that violence stems from high (or exaggerated) self-esteem (Baumeister, Smart & Boden, 1996; Barri et al., 2007; Bushman & Baumeister, 1998; Lambe et al., 2018; Maples et al., 2010). Or, as these authors interpret, violence arises from "wounded pride", from the motivation to seek validation (Baumeister,

Smart & Boden, 1996; Baumeister, Bushman, & Campbell, 2000). Narcissistic people who have a high opinion of themselves (high self-esteem) expect others to share the same opinion and can show aggression when they feel a threat to their ego, i.e. a threat to their self-esteem. Actually, these authors point out that they see narcissism as a risk factor that can cause aggression upon provocation rather than a direct causal relationship between narcissism and aggression (Bushman & Baumeister, 1998).

Authors who point out numerous contradictions in the premise that low self-esteem is the cause of violence also refer to works on the psychology of terrorism. Thus, they criticize different conclusions about the most common personality traits of terrorists, among which those that characterize terrorists "low self-esteem and tendency to take risks" (Long, 1990, according to Bushman & Baumeister, 1998: 18). Namely, the authors claim that Long's explanation of low self-esteem corresponds more to the description of high self-esteem, since it is estimated that these individuals tend to set unrealistic goals, and that after facing failure, they do not reduce their aspirations towards those goals, but rather raise them. It is this argument that increasing striving and taking greater risks after failure is a reflection of high, not low self-esteem, that led the authors to conclude that violent patterns indicate high, rather than low, self-esteem (Baumeister, Heatherton & Tice, 1993). These authors also argued in their works for revising the one-sided positive view of self-esteem. According to them, instead of the term self-esteem, the term egoism can be used, which fundamentally combines the concepts of pride, arrogance, conceit, narcissism and a sense of superiority, as well as the need for admiration from others. Starting from the understanding of self-esteem as an individual's belief that he is a superior being, or that he evaluates himself extremely favorably (especially in comparison to other people), it seems to us a very valid statement of those authors who believe that if society does not influence the reduction and mitigation of the excessive egoism of the individual, that excessive egoism can be seen as one of the causes of increased violence (Baumeister, Smart & Boden, 1996).

Of course, self-esteem should not be seen as an independent and direct cause of violence, but in a way that high self-esteem combined with a threat to the ego can represent a risk for violent behavior. It is precisely the threat to the ego that is the most common form of provocation in persons with pronounced narcissism (Baumeister & Boden, 1998: 118). For narcissists, aggression serves as a means of defending their own (unrealistic) view of themselves. When the positive attitude about oneself is questioned, when it is challenged, contradicted by another, the narcissistic person can become violent and show aggression, usually towards the source of the threat. This happens because people are generally not ready to revise their self-esteem downward. That would be another argument in support of the opinion that people with high self-esteem will react more aggressively to the threat to ego. Namely, it has been shown that in interpersonal communications, people with low self-esteem more often avoid situations that can cause them to lose respect from

others, while those with high self-esteem do not avoid such situations because they do not anticipate that they will lose respect. But when threats to their self-esteem appear, they will react in ways that are often drastic and irrational. Argumentation for such conclusions can also be found in Swann's Theory of Self-Verification, according to which people resist changes in their own self-evaluation (Swann, 1987). In line with this theory, people who think something bad about themselves can be quite indifferent to positive evaluations given to them by others, while those who have a positive opinion of themselves will be very receptive to favorable feedback because it confirms their self-evaluations, and they will react quite strongly to unfavorable evaluations.

In any case, even if the authors look at self-esteem differently as a mediator in the relationship between narcissism and aggression, almost all of them share the same view that narcissistic people have unstable self-esteem (Cale & Lilienfeld, 2006). Based on this assumption, numerous studies have shown that narcissism is a predictor of aggression. A recent meta-analytic study that includes 437 independent studies finds that both "normal" and "pathological" narcissism are related to aggression, and that all three dimensions of narcissism (ie, true, grandiose, and vulnerable narcissism) are related to all forms of aggression (e.g., indirect, direct, physical, verbal...), and that the relationship is significant for both men and women, people of all ages, students and non-students, and people from individualist and collectivist countries. It has also been confirmed that provocation is a key moderator of the relationship between narcissism and aggression, i.e. that people with high narcissism are more prone to aggressive and violent reactions in provocative situations (Kjærvi & Bushman, 2021).

The findings of studies showing that narcissistic individuals have an attention bias, i.e. show hyper-vigilance to ambiguous signs of threat in their social environment, can be used to understand provocation as a cause of aggression (Reidy, Foster & Zeichner, 2010). Precisely because of this hypervigilance and the perception of a threat to their ego, and in the presence of other traits associated with narcissism (hostility, impulsivity), such persons will behave aggressively in situations that are uncertain or ambiguous.

As we know, the real world is undoubtedly full of uncertainty and ambiguous situations, so it is to be expected that narcissistic people will perceive such a world as an ego-threat and show unprovoked aggression. The same pattern of reaction to ego-threat was found in persons with manifested psychopathy, i.e. borderline personality disorder (Cale & Lilienfeld, 2006). Given that psychopathy by definition is characterized by easy entry into risky situations, a tendency to aggressive, impulsive reactions, i.e. poor control of behavior in potentially threatening situations (that is, situations that such persons interpret as threatening), it is not surprising that these persons can in certain situations display various forms of socially unacceptable behavior (Glenn, Kurzban, & Raine, 2011).

CONCLUDING CONSIDERATIONS

Undoubtedly, the social, political and economic circumstances in which people live reflect on their psychological functioning. Many authors agree that in modern society, especially individualistic cultures, the frequency of classic neurotic symptoms is decreasing, while the frequency of borderline disorders is noticeably increasing. This can be partly explained by faster social changes and modernization in contemporary Western culture, compared to collectivist cultures, where, as we have seen, individuals are less likely to develop borderline pathology. Perhaps this is because individuals in collectivist cultures have more protection from the family, or perhaps because these societies suppress the behavioral phenomena that characterize borderline personality disorder. It is noticeable that more research on aggression, narcissism, self-esteem comes from countries where individualism is more pronounced (most research was done in the United States, followed by Canada, the United Kingdom, Australia, etc.), and much less from countries that nurture collectivism. Therefore, we are left wondering if the phenomenon of self-esteem is more related to Western culture and why this is so. Is it because people from collectivist cultures have a different understanding of themselves, because social roles and relationships with others are much more important to them than the principle of individuality? Accordingly, if we have seen threatened self-esteem as a risk for aggression, what are the triggers for aggression in collectivistic cultures?

We can also look for explanations for the increase in narcissism in modern Western society in the increase in family, more specifically, parental dysfunction. We know that it is developmentally normal for children in a certain developmental period to have an unrealistic assessment of themselves and that their overall self-esteem is fragile at a young age. Most research on narcissism and aggression extrapolates their conclusions from studies conducted on youth populations. But we do not find enough explanation why some children already have a very early grandiose (mostly explicit) self-confidence, which often underlies their aggressive behavior. One of the theoretical assumptions is that the cause lies in dysfunctional parenting (whether it is extremely excessive parental praise of the child without a real basis, or parental rigidity, coldness and rejection). Available studies provide evidence for the assumption that such dysfunctional parent-child relationships will lead to increased narcissism (Carlson & Derde, 2009; Horton, Bleau, & Drvecki, 2006; Otvai & Vignoles, 2006).

Since we are witnessing not only the growth of individual narcissism but also the growth of collective narcissism, we consider it important to emphasize the issue of the responsibility of the community (society) towards human suffering, increasing tolerance towards sociopathological phenomena and immoral behavior, not cultivating empathy as a desirable and useful response in reconciliation processes. A society that is unable to take the perspective of victims, that uses the denial of group responsibility as a strategy to reduce guilt, that does not foster universal moral principles, and that ultimately (perhaps most tragically) dehumanizes those who are victimized, becomes itself dehumanized.

Finally, we believe that observing the manifestations of narcissism and aggressiveness from multiple perspectives can provide better insight into the mechanisms that drive the maladaptive interpersonal relationships of individuals with narcissistic and aggressive tendencies. As we have seen, threatened self-esteem affects the aggressive tendencies of narcissists, and it increases aggression in those with high self-esteem. But the question remains, what is beneath the inflated self-confidence, is there actually a deep feeling of insecurity hidden behind that grandiosity? And how much does a society in which the most powerful protagonists are individuals with an obvious borderline personality structure contribute to the overall feeling of insecurity? If we don't want to live in a borderline disturbed world, maybe to begin with we should stop supporting the positive illusions of narcissists that they are omnipotent, perfect and untouchable.

REFERENCE LIST

- Am. Psychiatr. Assoc 2013. *Diagnostic and Statistical Manual of Mental Disorders*. Arlington, VA: Am. Psychiatr. Publ, 5th ed.
- Bartholow, B. D., Sestir, M. A., & Davis, E. B. (2005). Correlates and consequences of exposure to video game violence: Hostile personality, empathy, and aggressive behavior. *Personality and social psychology bulletin*, 31(11), 1573-1586.
- Bandura, A., & Walters, R. H. (1977). *Social learning theory* (Vol. 1). Prentice Hall: Englewood cliffs.
- Baumeister, R. F., Bushman, B. J., & Campbell, W. K. (2000). Self-esteem, narcissism, and aggression: Does violence result from low self-esteem or from threatened egotism? *Current directions in psychological science*, 9(1), 26-29.
- Baumeister, R. F., Smart, L., & Boden, J. M. (1996). Relation of threatened egotism to violence and aggression: the dark side of high self-esteem. *Psychological review*, 103(1), 5.
- Baumeister, R. F., Heatherton, T. F., & Tice, D. M. (1993). When ego threats lead to self-regulation failure: negative consequences of high self-esteem. *Journal of personality and social psychology*, 64(1), 141.
- Baumeister, R. F., & Boden, J. M. (1998). Aggression and the self: High self-esteem, low self-control, and ego threat. In *Human aggression* (pp. 111-137). Academic Press.
- Bettencourt, B., Talley, A., Benjamin, A. J., & Valentine, J. (2006). Personality and aggressive behavior under provoking and neutral conditions: a meta-analytic review. *Psychological bulletin*, 132(5), 751.
- Blais, J., & Pruyers, S. (2017). The power of the dark side: personality, the dark triad, and political ambition. *Personality and Individual Differences*, 113, 167-172.
- Bushman, B. J., & Anderson, C. A. (1998). Methodology in the study of aggression: Integrating experimental and nonexperimental findings. In *Human aggression* (pp. 23-48). Academic Press.

Bushman, B. J., & Baumeister, R. F. (1998). Threatened egotism, narcissism, self-esteem, and direct and displaced aggression: Does self-love or self-hate lead to violence? *Journal of personality and social psychology*, 75(1), 219.

Cale, E. M., & Lilienfeld, S. O. (2006). Psychopathy factors and risk for aggressive behavior: A test of the “threatened egotism” hypothesis. *Law and human behavior*, 30, 51-74.

Caprara, G. V., Barbaranelli, C., Consiglio, C., Picconi, L., & Zimbardo, P. G. (2003). Personalities of politicians and voters: Unique and synergistic relationships. *Journal of Personality and Social Psychology*, 84(4), 849.

Caprara, G. V., & Zimbardo, P. G. (2004). Personalizing politics: a congruency model of political preference. *American psychologist*, 59(7), 581.

Campbell, W. K., Rudich, E. A., & Sedikides, C. (2002). Narcissism, self-esteem, and the positivity of self-views: Two portraits of self-love. *Personality and Social Psychology Bulletin*, 28(3), 358-368.

Campbell, W. K., Rudich, E. A., & Sedikides, C. (2002). Narcissism, self-esteem, and the positivity of self-views: Two portraits of self-love. *Personality and Social Psychology Bulletin*, 28(3), 358-368.

Campbell, W. K., & Miller, J. D. (2011). *The handbook of narcissism and narcissistic personality disorder* (pp. 309-318).

Czibor, A., & Bereczkei, T. (2012). Machiavellian people’s success results from monitoring their partners. *Personality and Individual Differences*, 53(3), 202-206.

Dodge, K. A. (2006). Translational science in action: Hostile attributional style and the development of aggressive behavior problems. *Development and psychopathology*, 18(3), 791-814.

Donnellan, M. B., Trzesniewski, K. H., Robins, R. W., Moffitt, T. E., & Caspi, A. (2005). Low self-esteem is related to aggression, antisocial behavior, and delinquency. *Psychological science*, 16(4), 328-335.

Divac Jovanović, M., & Švrakić, D. (2016). *Granična ličnost i njena različita lica: šta su poremećaji ličnosti*. Beograd: Clio.

Djurdjevic, S., Boskovic, M., Djurdjevic, A., & Misev, G. (2022). Brain as a Social Organ. In *Regulating Human Rights, Social Security, and Socio-Economic Structures in a Global Perspective* (pp. 63-81). IGI Global.

Djurdjevic, S., Krivokapić, Z., Shapic, R., & Vicentic, S. (2016). Understanding conative regulation systems—an examination of the differences between offenders and non-offenders. *Journal of Special Education and Rehabilitation*, 17(1-2), 66-84.

Đurđević, S. Vrednosne orijentacije i granični poremećaj ličnosti, 25. SEMINAR „LJUDI GOVORE“ u organizaciji Udruženja „Čovek i psiha – Man and Psyche”, Tema: “Granice granica”, Beograd, 08.06.2023, (proceedings in print).

- Ellison, W. D., Rosenstein, L. K., Morgan, T. A., & Zimmerman, M. (2018). Community and clinical epidemiology of borderline personality disorder. *Psychiatric Clinics*, 41(4), 561-573.
- Fine, R. (1986). *Narcissism, the self, and society*. Columbia University Press.
- Goodman, M., & New, A. (2000). Impulsive aggression in borderline personality disorder. *Current psychiatry reports*, 2(1), 56-61.
- Glenn, A. L., Kurzban, R., & Raine, A. (2011). Evolutionary theory and psychopathy. *Aggression and violent behavior*, 16(5), 371-380.
- Hart, W., Richardson, K., & Tortoriello, G. K. (2018). Dark personality voters find dark politicians more relatable and fit for office. *Journal of Research in Personality*, 75, 59-68.
- Heine, S. J., & Hamamura, T. (2007). In search of East Asian self-enhancement. *Personality and Social Psychology Review*, 11(1), 4-27.
- Huesmann, L.R., & Guerra, N.G. (1997). Children's normative beliefs about aggression and aggressive behavior. *Journal of Personality and Social Psychology*, 72, 408-419.
- Kajonius, P. J., Persson, B. N., & Jonason, P. K. (2015). Hedonism, Achievement, and Power: Universal values that characterize the Dark Triad. *Personality and Individual Differences*, 77, 173-178.
- Kowalski, C. M., Kwiatkowska, K., Kwiatkowska, M. M., Ponikiewska, K., Rogoza, R., & Schermer, J. A. (2018). The Dark Triad traits and intelligence: Machiavelians are bright, and narcissists and psychopaths are ordinary. *Personality and Individual Differences*, 135, 1-6.
- Kjærviik, S. L., & Bushman, B. J. (2021). The link between narcissism and aggression: A meta-analytic review. *Psychological bulletin*, 147(5), 477.
- Kujačić, D., Međedović, J., Knežević, G. (2015). The relations between personality traits and psychopathy as measured by ratings and self-report. *Psihologija*, 48(1), 45-59.
- Knežević, G. (2003). *Koreni amoralnosti*. Beograd: Centar za primenjenu psihologiju i Institut za kriminološka i sociološka istraživanja.
- Lasch, C. (2019). The Culture of Narcissism. In *American Social Character* (pp. 241-267). Routledge.
- Lambe, S., Hamilton-Giachritsis, C., Garner, E., & Walker, J. (2018). The Role of Narcissism in Aggression and Violence: A Systematic Review. *Trauma, Violence, & Abuse*, 19(2), 209-230.
- Lilienfeld, S. O., Waldman, I. D., Landfield, K., Watts, A. L., Rubenzer, S., & Faschingbauer, T. R. (2012). Fearless dominance and the US presidency: implications of psychopathic personality traits for successful and unsuccessful political leadership. *Journal of personality and social psychology*, 103(3), 489.

Malamuth, N. M., Linz, D., Heavey, C. L., Barnes, G., & Acker, M. (1995). Using the confluence model of sexual aggression to predict men's conflict with women: a 10-year follow-up study. *Journal of personality and social psychology*, 69(2), 353.

Međedović, J. (2009). Bazična struktura ličnosti i kriminalitet. *Primenjena psihologija*, 2(4), 339-367.

Paulhus, D. L., & Williams, K. M. (2002). The dark triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of research in personality*, 36(6), 556-563.

Patton, C. L., Smith, S. F., & Lilienfeld, S. O. (2018). Psychopathy and heroism in first responders: Traits cut from the same cloth? *Personality Disorders: Theory, Research, and Treatment*, 9(4), 354.

Radulović, D. (2006). *Psihologija kriminala – psihopatija i kriminal*. Beograd, Fakultet za specijalnu edukaciju i rehabilitaciju i institut za kriminološka i sociološka istraživanja.

Reiss, S. (2004). Multifaceted nature of intrinsic motivation: The theory of 16 basic desires. *Review of general psychology*, 8(3), 179-193.

Reidy, D. E., Foster, J. D., & Zeichner, A. (2010). Narcissism and unprovoked aggression. *Aggressive Behavior*, 36(6), 414-422.

Rodkin, P. C., Farmer, T. W., Pearl, R., & Van Acker, R. (2006). They're cool: Social status and peer group supports for aggressive boys and girls. *Social Development*, 15(2), 175-204.

Sestir, M. A., & Bartholow, B. D. (2007). Theoretical explanations of aggression and violence. Aggressive offenders' cognition: *Theory, research, and practice*, 155-178.

Shirokova, G., Galieva, N., Doktorova, D., White, J. V., & Marino, L. (2024). Strategic entrepreneurial behaviors and firm performance: The moderating role of narcissism and Machiavellianism. *Journal of Small Business and Enterprise Development*, 31(1), 191-225.

Smith, M. B., Hill, A. D., Wallace, J. C., Recendes, T., & Judge, T. A. (2018). Upsides to dark and downsides to bright personality: A multidomain review and future research agenda. *Journal of Management*, 44(1), 191-217.

Sutherland, E. H. (1972). The theory of differential association. In *Readings in criminology and penology* (pp. 365-371). Columbia University Press.

Swann, W. B. (1987). Identity negotiation: Where two roads meet. *Journal of personality and social psychology*, 53(6), 1038.

Teng, Z., Liu, Y., & Guo, C. (2015). A meta-analysis of the relationship between self-esteem and aggression among Chinese students. *Aggression and violent behavior*, 21, 45-54.

Watts, A. L., Lilienfeld, S. O., Smith, S. F., Miller, J. D., Campbell, W. K., Waldman, I. D., & Faschingbauer, T. J. (2013). The double-edged sword of grandiose nar-

cissism: Implications for successful and unsuccessful leadership among US presidents. *Psychological science*, 24(12), 2379-2389.

Walker, J. S., & Bright, J. A. (2009). False inflated self-esteem and violence: A systematic review and cognitive model. *The Journal of Forensic Psychiatry & Psychology*, 20(1), 1-32.

Zeigler-Hill, V., & Besser, A. (2013). A glimpse behind the mask: Facets of narcissism and feelings of self-worth. *Journal of personality assessment*, 95(3), 249-260.

Zhang, L., & Zhu, H. (2021). Relationship between narcissism and aggression: A meta-analysis. *Acta Psychologica Sinica*, 53(11), 1228.

Dejan Labović¹
Zoran Marjanović²

THE ROLE OF THE PRIVATE SECURITY SECTOR IN THE PREVENTION OF INTERSTATE CONFLICTS

Abstract

Globalization and the complexity of the modern world have made it increasingly difficult to recognize the dangers and risks of society, which are increasingly unpredictable in time and space, and multidisciplinary complex without the ability to comprehensively and effectively control them, and to which traditional management models characteristic of national security systems do not have an adequate response. At the same time, conflicts have become more complex and long-lasting, the nature, intensity and frequency of which have evolved in recent years, moving from conflicts that are fought directly between states to various forms of internal or intrastate violence. They are increasingly connected to global challenges and risks of society, which are most often economic, political, security, technological, demographic, environmental, health, etc. As a result of all this, new concepts and attitudes are being incorporated into the national security strategies of modern states that recognize the new reality of redefining the role of national security, through the privatization of state security functions and a multi-centric perspective of society towards current risks, their prevention and control, as a potential solution for managing future conflicts and crises. The paper indicates that, given the background of conflict situations, the private security sector, with appropriate support from national actors, represents an important segment for conflict prevention, through preventive integrative security operations and joint policies, as well as through appropriate mechanisms for the immediate reconstruction of society and peacebuilding.

Keywords: *interstate conflict, prevention, danger, risk, concept of security, private security sector.*

¹ Faculty of Diplomacy and Security, Belgrade, Serbia, labovicdejan@gmail.com

² Military Security Agency, Belgrade. Serbia

INTRODUCTION

Since the end of the Cold War, it has been recognised that conflicts¹ have been largely confined to developing countries and have often taken the form of intra-state rather than inter-state conflicts, with incalculable consequences for many states (Government UK 2015:29). While the world is changing rapidly and fundamentally, driven by long-term shifts in the balance of global economic and military power, with increasing competition between states, conflicts have now become fluid and protracted, taking place against a backdrop of local conflicts, involving multiple non-state groups and regional and international actors, and are often "asymmetrical", "hybrid", "informal", and "low-intensity".²

Conflicts are often linked to global challenges, from climate change to transnational organized crime, with enormous social and economic costs, displacement and long-term humanitarian needs, the negative effects of which often spread to nearby regions and, in some cases, even globally. Namely, the nature, intensity and frequency of conflicts have evolved in recent years, moving from wars fought directly between states, to various forms of "internal" or intra-state violence, including insurgencies, guerrilla warfare, terrorism, large-scale organized and criminal violence and protests, which increase corruption and weaken state institutions.

Most of these conflicts have had an ethnic or religious overtone, and were most often fueled by competition over natural resources, for example since 2010 the number of conflicts in the world has been increasing, with more countries experiencing violent conflict in 2016 than at any time in almost 30 years. Around two out of eight billion people currently live in countries affected by conflict. There are currently several high-intensity conflicts ongoing and around 70 conflicts are low-intensity violent conflicts (World Bank and United Nations 2018:32). Conflicts cost an estimated \$13.6 trillion each year and pose a significant threat to the UN's 2030 Agenda for Sustainable Development and Peace (UNSC Resolution 2282 and A/RES/70/262). After conflict, a nation's highest priorities are often building peace, stability, and accelerating economic growth.

¹ Conflict most often represents unilateral physical violence against civilians (e.g. genocide), as well as various repressive social relations that cause death and human suffering (e.g. apartheid), and is always long-term and based on real social causes of disagreement, with its phases: the early phase of manifest latent tension, the crisis phase, the violent phase, and the post-conflict phase, See: Uppsala Universitet – Department of Peace and Conflict Research: Definitions (2011), p. 33. <http://www.pcr.uu.se/research/ucdp/definitions/>.

² It is evident that the entire history of society is permeated with conflict. The first half of the twentieth century will be remembered for two world wars, while the second half of the twentieth century and the beginning of the twenty-first century are characterized and marked by a large number of regional and local armed conflicts. See: Haider, H. (2014). *Conflict: Topic Guide*: Chapter 3: Preventing and Managing Violent Conflict, Governance and Social Development Resource Centre, p. 57.

According to the World Bank's annual World Development Report 2023³, most conflicts occur in developing countries that have limited capacity to address humanitarian crises and post-conflict recovery and reconstruction. According to the report, in order to stabilize conflict situations in the long term, states have the primary responsibility for preventing them, but for them to be effective, civil society, the private sector, regional and international organizations must be important partners in preventing and resolving conflicts, providing humanitarian assistance, and post-conflict reconstruction of society (World Bank Flagship Report, 2023: 35).

Given that conflict is the result of intersecting factors in different ways⁴, which have complex socio-cultural, economic and political dimensions, conflict prevention is an important and complex process, which requires a timely and adapted approach in each context, i.e. a combination of a good knowledge of the actual circumstances on the ground and a good overview of the available tools and approaches for conflict prevention. Such conflict prevention must be based on the activities of constant conflict analysis,⁵ with the aim of identifying patterns and dynamics of conflict, and its future prospects, with conflict analysis essentially being accepted as a continuous and reflexive process involving multiple stakeholders and perspectives, with recognition of the context of the root causes of conflict and an adapted approach and management for each conflict context. An indispensable factor in conflict prevention is strengthening the potential for conflict prevention, through the continuous strengthening of local capacities for peace (resources, structures, attitudes, skills), early warning systems, and the development of long-term international cooperation.

The global context and the human and economic cost of violent conflicts around the world require more collaborative work and inclusive solutions, where the private security sector is increasingly seen as an important national and international partner in the prevention and resolution of violent conflicts (Lund, 2009: 29). There is a consensus in the international community that the contribution of the private security sector should

³ World Bank research shows that half of developing countries that have experienced conflict return to war within five years of a peace agreement, as weak governments lack the necessary capacity, meaning that if reconstruction fails, poverty increases and frustrations grow, leading to a lack of trust in institutions and a general decline in economic activity. *World Bank Flagship Report* (2023), p. 62.

⁴ Identifying income disparities, the security environment, the proliferation of weapons and military technology, cultural inequalities and multidimensional forms of poverty between regions and national communities, resources whether food, energy, water or raw materials, are the most common contemporary factors of increasing interstate tensions, i.e. overt or covert reasons for armed conflicts. See: International Alert (2015) *Building prosperity and peace: Integrating peacebuilding into economic development*, London: International Alert, p. 34

⁵ Conflict analysis should be seen as an ongoing and reflective process of identifying contextual perspectives and approaches to conflict resolution, which include inclusive economic and social policies and effective institutions. Haider, H. (2014). *Conflict: Topic Guide*: Chapter 3: Preventing and Managing Violent Conflict, Governance and Social Development Resource Centre, p. 11.

be an integral part of the institutional efforts of post-conflict countries, through risk-sharing mechanisms, public-private partnerships in the reconstruction of society and the building of a functional state. On the other hand, the engagement of the private security sector through non-state actors has simultaneously posed a particular challenge to international peacebuilding efforts, due to the potential dangers of achieving their political and/or economic goals (Carayannis, 2018: 38).

Contemporary Features and Prevention of Interstate Conflicts

Interstate conflict is not a new phenomenon. Throughout history, interstate conflicts have killed tens of millions of people, displaced entire communities, caused trillions of dollars in destruction, and contributed to the spread of hunger, poverty, and disease. Interstate conflict is among the greatest threats to world order, as the potential devastation of war has increased since the introduction of nuclear weapons at the end of World War II, as full-scale war could spell the end of civilization itself. The prelude to today's interstate conflicts are current security challenges, such as uncertainty, instability, and conflicts fueled by regional and local tensions, the roots of which are most often historical animosity, attempts at regional hegemony, ethnic, religious, or other forms of shared hostility, control over resources, capitalization of global technology, proliferation of weapons and military technology, fluidity of territorial borders of states, alienation between entities, etc. (Krause, 2016: 33).

The good news is that interstate conflicts have declined since the end of World War II, with global trends indicating that they are declining relative to intrastate conflicts, due to the development of peaceful developments and the end of bipolar rivalry, bringing about a significant shift in the perception of such security issues and alternative approaches.⁶ This trend is a result, on the one hand, of the low probability that modern democracies will fight each other and that increased international trade has made the world a safer place, as economically interdependent countries are less likely to go to war, and responsible leaders are less willing to wage potentially costly and unpopular wars (Peace Research Institute Oslo PRIO, 2018: 46). On the other hand, powerful alliances such as the North Atlantic Treaty Organization (NATO) can deter interstate war, and international institutions such as the United Nations also provide forms for states to peacefully resolve conflicts, while acknowledging the fact that these institutions cannot completely prevent conflicts, for example the ongoing war in Ukraine (SIPRI-UNESCO Handbook, 1998: 13-25).

⁶ Conflicts between states and their allies accounted for over 40% of all conflicts during the Cold War. If economic crises, with the challenges of transition, prevail in the coming decades, the frequency of interstate conflicts will increase dramatically, given that economic development is strongly linked to the stability of societies. See: *UN Global Study on the implementation of the UN Security Council Resolution 1325*: (2015) "Preventing Conflict, Transforming Justice, Securing the Peace", p.77.

In such global relations of distant harmony, forms of interstate conflicts in some cases have the international character of violent conflicts, the modern hallmark of which is a conflict between two countries (e.g. Eritrea and Ethiopia - 1998) or the participation of several countries (Israeli-Arab wars where participants at different times were Israel, Egypt, Syria, Palestine, Jordan, Iraq), involving armed force, and financial and human resources to achieve goals. In recent years, China has continued to threaten to use force to achieve unification with Taiwan. The United States has also used armed force to achieve various interests abroad, including combating terrorist threats, resolving humanitarian crises, and overthrowing unfavorable regimes. Among other goals, military operations can also be conducted in self-defense, to stop civil unrest and to secure access to economic resources (Watts, 2017: 51).

In other cases, forms of interstate conflicts have the internal character of non-violent conflicts, which are most often less violent than conventional conflicts, but pose a direct undermining of rivals and a significant risk to property, people and their governments (Szayna et al., 2018: 37). Such conflicts are all conflicts within the territory of a state with the aim of changing power, secession of part of the territory or the defense of basic human freedoms, religious and ideological rights and can be conducted in the form of secessionist, civil, guerrilla, military and state coups, and terrorism, the number of which is growing alarmingly (almost 90% of all conflicts).

These conflicts, as a form of internal, interstate conflict, are carried out through a range of economic, environmental, diplomatic, and cyber tools, with the aim of increasing power and advancing national interests. *Economic sanctions*, as an alternative to war, are used by countries to force individuals, companies, and governments to change their behavior on a wide range of issues, including human rights. They can have devastating consequences by cutting off countries' access to food, energy, and financial resources, but they rarely force a country to fundamentally change course.⁷ It is estimated that US sanctions have cost Cuba about \$130 billion over the past sixty years, a figure far greater than the entire Cuban economy (\$100 billion in 2018). *Environmental threats* can contribute to food and water shortages, especially as global temperatures rise and ecosystems become increasingly vulnerable. Countries can manipulate shared ecosystems, such as rivers and forests, to benefit themselves or to intentionally harm their neighbors.⁸ Instead of going to war directly, powerful countries can fight each other by financing or arming opposing sides in a third country, so-called "*proxy wars*"

⁷ The US has imposed sanctions on Cuba, Iran and North Korea and bears the brunt of Iranian and Russian interference in their elections. See also: United Nations and World Bank Flagship Study (2016); *Sustaining Peace: making Development Work for Prevention of Violent Conflicts*, Concept Note, October 13, p. 12.

⁸ Ethiopia's construction of a dam on the Nile River threatens Egypt's vital water source, which supports nearly all of the country's 100 million people. Egypt has threatened military action to combat the ecological threat posed by the dam. Ibid, p.21.

(Von Einsiedel et al., 2017: 25). The Middle East has been host to several "*proxy wars*" in which two regional powers have largely refrained from full-scale war, most notably Iran and Saudi Arabia, which have financed, trained, and equipped the opposing sides, contributing to hundreds of thousands of deaths in Syria and millions of starvation in Yemen. The USA and Russia (then the USSR) after the Cold War waged "*proxy hot wars*" from all-out invasions to limited covert assistance in Afghanistan, Angola, Cuba, Chile, Nicaragua, Congo, Vietnam and Korea, which claimed millions of lives and resulted in political dilemmas that are still evident today. Now in Syria, the open military interventions of Western powers on the one hand and Russia on the other, the support of Iran, the interference of Israel, have shown the intertwining of the causes of the conflict: political (change of power and state structure), anti-terrorist (fight against the Islamic militant group ISIS) and energy causes (direction of development of gas and oil pipelines) (Von Einsiedel et al., 2017: 33); *Destabilizing an opposing government*, through election interference, diplomatic confrontations⁹, supporting or arming opposition, separatist, or terrorist groups, through covert operations and intelligence gathering. India and Pakistan, for example, have long accused each other of supporting separatist groups in troubled areas of their countries; Finally, *cyberattacks*¹⁰ target the adversary's infrastructure and vital facilities, using technology that allows countries to attack adversary's computer systems covertly, from afar, and with relatively little risk (Szayna et al., 2018: 44).

In order to properly approach conflict resolution¹¹, we must first understand it. The first step towards understanding and resolving a conflict is its detailed analysis,

⁹ Bahrain, Egypt, Saudi Arabia, and the United Arab Emirates severed ties with Qatar in 2017 over allegations of funding terrorism, closing Qatari embassies in their countries, and banning Qatari aircraft from their airspace. Ibid, p.33.

¹⁰ In 2017, Chinese hackers stole the Social Security numbers of over 145 million Americans after an attack on credit reporting agency Equifax. Tensions over cyberwarfare escalated into a diplomatic standoff in 2020 when the United States ordered China to close its consulate in Houston over allegations of Chinese espionage and intellectual property theft. In retaliation, China closed the U.S. consulate in Chengdu. This cut off U.S. access to nearby Tibet, where the United States has accused China of human rights abuses. None of these issues led to all-out war, but the escalation of tensions between the world's two most powerful economies has serious political and financial implications, Ibid, p. 27.

¹¹ Conflict resolution refers to all processes and methods of resolving conflict, dealing with the underlying causes of conflict, whether between individuals, groups or states. More: Kevin Avruch, (2009) "Culture theory, culture clash, and the practice of conflict resolution", in: Dennis J. D Sandole, Sean Byrne, Ingrid Sandole and Jessica Senehi (eds.), *Handbook of Conflict Analysis and Resolution*, p. 24.

given that each conflict is based on different causes¹² of disagreement and animosity. Conflict analysis is a continuous and reflective process of systematically studying the profile, causes, actors and dynamics of conflict. Namely, conflict analysis is a cycle of research and understanding the conflict reality from different perspectives, involving multiple stakeholders and positions, in order to identify the needs, interests, positions, power and resources among potential connecting factors and actors of violence. Conflict analysis can be conducted at different levels (local, regional, national, etc.) and seeks to establish connections between these levels (Fisher (ed) 2000: 17).

For decades, the world has been dominated by a conflict-response approach to peace and security, with conflict prevention remaining under-prioritized and under-funded. However, there is growing recognition that conflict prevention¹³ is a complex process of using a variety of methods, approaches and mechanisms of engagement, initiatives and activities to prevent, resolve or re-open conflict, and to measure its outcomes (CPPAC-END-NOTES, 2015: 23). Essentially, conflict prevention is always linked to conflict management¹⁴, conflict resolution and peacebuilding¹⁵, through the promotion of social, economic and political inclusion. The aforementioned conflict prevention activities aim to reduce manifest tensions and prevent the outbreak of recurrent conflicts, including a variety

¹² There are essentially two types of causes of conflict: fundamental (root) or structural causes and immediate or proximate causes. Root causes stem from a general structural or deep-rooted background, they are underlying events and conditions that have existed for many years and are generally changing slowly and are most often politically instrumentalized, and can be embedded in historical and cultural contexts such as religious conflicts, long-standing border disputes, difficulties in state-building, poverty and economic exclusion or environmental degradation. Immediate causes relate to medium-term and emerging socio-political conditions and economic developments. Examples of immediate causes are human rights violations, trends in income inequality, political repression, etc. , where citizens respond violently to a lack of freedom, democracy and to policies of discrimination, exclusion, poor governance and dictatorship. See: *Economic and Political Causes of Conflict: An Overview and Some Policy Implications*, CRISE, University of Oxford, Working Paper No. 81, February 2015 12 See Denney, L Mallett, R & Mazurana, D (2015), p. 33.

¹³ Conflict prevention includes early warning measures, confidence-building activities, security, strong encouragement of an inclusive environment, preventive deployment of peacekeeping forces and can be undertaken before the escalation of conflict or after the establishment of peace, in order to prevent the recurrence of conflict. More: Michael S. Lund (2009): *Conflict Prevention: Theory in Pursuit of Policy and Practice*, The Sage Handbook on Conflict Resolution, p. 33, and Alex P. Schmid, (1998) *Thesaurus and Glossary of Early Warning and Conflict Prevention Terms*, Synthesis Foundation, p. 12.

¹⁴ Conflict management is the process of containing, mitigating, limiting, deescalating, and transforming conflict. See: Kevin Avruch, (2009) "Culture theory, culture clash, and the practice of conflict resolution", in: Dennis J. D Sandole, Sean Byrne, Ingrid Sandole and Jessica Senehi (eds.), *Handbook of Conflict Analysis and Resolution*, p. 247.

¹⁵ Peacebuilding is the restoration of normal socio-economic relations between former conflicting parties, as well as the identification of the relations and social context that gave rise to the conflict. For more information: Yaacov Bar-Siman (2004): *Why Reconciliation?* in: Yaacov Bar-Siman - (ed.), *From Conflict Resolution to Reconciliation*, p. 3-4.

of confidence-building measures, measures to resolve specific grievances, measures to address the root causes of conflict (poverty reduction, democracy building, etc.), including diplomacy, mediation and institution building. While conflict prevention initiatives include early prevention initiatives (improving relations between parties before violent conflicts break out) and late prevention initiatives (resolving or preventing the recurrence of violent conflicts) and are implemented at the local or international level (Schmidt, 1998: 12).

However, within the framework of the application of direct methods, approaches and mechanisms of engagement in conflict prevention, it is most often categorized as direct, structural and systemic prevention (CPPAC-ENDNOTES, 2015: 26). *Direct conflict prevention* refers to short-term initiatives (e.g. dialogue, mediation and other confidence-building measures, preventive international deployment and the establishment of peace zones) that are put in place at a critical moment with the aim of having a direct de-escalating effect on tensions or violence. *Structural conflict prevention* represents the most relevant aspect of conflict prevention, it refers to long-term initiatives to address the root causes of tensions and violence, in the early (or latent) phase of the conflict, which aim to transform the key socio-economic sources of conflict, through development cooperation in different sectors of society (Lund, 2009: 33). As for *systemic conflict prevention*, it essentially represents a holistic approach to conflict prevention at the regional level, which includes early warning systems¹⁶, interagency cooperation, and the exchange of data and experiences (CPPAC-ENDNOTES, 2015: 26).

Therefore, it is concluded that current trends and drivers of interstate conflicts (the global context of a multipolar world, with new centers of military and economic power) intersect in complex ways and contribute to the complexity of conflict. Faced with such geopolitical fluidity, the inevitable response that provides channels and incentives for calming conflict before it escalates to the level of widespread violence is: the rise of effective international mechanisms for conflict mediation (in particular, peacekeeping operations authorized by the United Nations - UN), with information about the risk of conflict; the spread of national democratic forms of government, together with a credible threat of external intervention (most often by great powers, especially the USA); and increasing support for national and regional conflict prevention programs, with integration into development strategies and investment in sustainable social development and more inclusive institutions.

¹⁶ An early warning system has four components: information gathering (using specific indicators of the causes of conflict); information analysis (putting conflict indicators into context, recognizing the development of the crisis); formulating best and worst case scenarios for the crisis (considering options for responding to the crisis); and communication with all actors involved in emergency planning (sharing and assessing available information). See also Ulrich Schneckener, 'Dealing with armed non-state actors in state- and peace-building: types and strategies', in Wolfgang Benedek, Christopher Daase, and Petrus Van Dyne (eds), *Transnational Terrorism, Organised Crime and Peace-building*, Palgrave, Basingstoke, (2010), pp. 229–248.

Specificities of the private security sector in the prevention of interstate conflicts

In the formation of a global security network, the international community is undergoing a transformation in the way security is managed, where with the change in the nature of modern peacekeeping, the privatization of the security sphere with the commercial-contractual potential for achieving human security is also emerging. Namely, if today traditional wars are replaced by non-classical and non-state conflicts that are associated with modern challenges and threats, then traditional peacekeeping operations are also going through a process of adaptation to the new reality, that is, peacekeeping is looking for non-traditional ways to resolve conflicts, using new means at their disposal.

The growth of peacekeeping activities came as a consequence of the fact and the need for consensual settlements around the world, because numerous violent conflicts were previously most often contained through the intermediary participation of superpowers. Specifically, new conflicts, whether "asymmetric", "hybrid", "informal", "low-intensity", etc., require non-traditional ways of resolving conflicts and sophisticated logistical support (construction of bases, camps and field offices, guarding and security, etc.), i.e. peacekeeping requires that the private security sector be part of the tools available to UN peacekeeping missions (Avruch, 2009: 247).

Given that the complex nature of post-conflict situations has left governments with few market alternatives, as military forces have become specialized and unable to cope with the range of tasks associated with post-conflict operations, a new set of institutional arrangements has gradually emerged to manage complex multilateral interventions, of which stabilization operations and post-conflict reconstruction are vital parts. In such post-conflict arrangements, planning and execution must be coordinated between government agencies, non-governmental organizations, international organizations and the private security sector. Thus, in addition to traditional peacekeeping functions, new efforts are needed to implement peace, i.e. an increase in the number of new missions is required, which has created a number of tasks: election observation, refugee assistance and repatriation, human rights protection, training, demining, humanitarian assistance, disarmament of military and paramilitary groups, etc. (D. Sandole, 2000: 3–6). This has led to the increasing privatization of traditional domains of the state and the rise in the need for the private security sector to have an increasing influence in the international community and be part of the tool available to UN peacekeeping missions. Another reason for the privatization of traditional domains of the state in post-conflict missions is the rapid growth in the number of international personnel working for international non-governmental organizations and multilateral organizations and companies that have arrived in the conflict zone for the purpose of post-conflict transition and reconstruction programs (Nakarada and Baljetbo, 2007: 12).

In the context mentioned above, the goal of peacekeeping is always to reduce violence and the threat of violence, for the sake of human safety and security, and is

one of the main instruments of overall human security. Although there is no single definition of peacekeeping in theory¹⁷, in the UN Charter, peacekeeping falls under six basic categories: *conflict prevention*, *peacemaking*, *peacekeeping*, *peace enforcement*, *post-conflict reconstruction and peacebuilding*. The first three categories (conflict prevention, peacemaking, peacekeeping) make up Chapter VI of the UN Charter, and are implemented with the consent of the parties to the conflict, the impartiality of UN forces and the impossibility of the use of force. While the category of *peacekeeping* includes military intervention, where the consent of the parties to the conflict is not necessary, impartiality is conditional and the use of force is permitted only under certain conditions determined by the UN Security Council. The category of *peacebuilding* falls under Chapter VII of the UN Charter and is permitted only by decision of the UN Security Council, in situations of need to restore international peace and security, as well as in situations of threat to the peace, breach of the peace, or act of aggression.¹⁸

When the UN Security Council decides to intervene militarily, the peacekeeping force is selected, where the UN Security Council decides, but not necessarily, which troops will be used and how they will be used to resolve the conflict. However, to date, the UN Security Council has most often considered the use of private security companies for peacekeeping missions, only when peacekeeping troops were not available, nor were troop-contributing countries quick enough to deploy military personnel on the ground and stop the violence (Gowan, 2012: 47). In this situation, the impression is that the global private security industry is part of a broader trend of stabilization operations and post-conflict reconstruction, which suggests an increasing and more immediate acceptance and use of private security sector companies (PSSCs) in post-conflict environments, through commercial security firms¹⁹ (private military companies - PMCs²⁰ and

¹⁷Peacekeeping is "containment and mitigation of conflict" rather than "resolving the sources of conflict", which requires impartiality and neutrality, control and accountability, oversight and transparency, legitimacy, cost and efficiency. See: <http://www.un.org/en/charter-united-nations/>.

¹⁸More: <http://www.un.org/en/charter-united-nations/>.

¹⁹Private security providers exhibit a "hybrid organizational form" in their organizational activities, ranging from combat and operational support, military advice and training, weapons procurement, intelligence gathering, security services, diplomatic protection for large corporations, NGOs and the UN, crime prevention and logistical support. More than 90% of the private security industry provides logistical support or training, rather than armed security. To date, approximately 2,800 private security companies have operated in South Africa. See: International Stability Operations Association (ISOA), formerly known as the International Peacekeeping Operations Association (IPOA).

²⁰The participation of PMCs in peacekeeping missions can be divided into two types: active ones that implement low-intensity military operations, with training, and passive ones that do not accompany their clients into the field and do not engage in deadly combat. An example of a passive PMC is the American PMC "MPRI" that conducts consultations and training around the world, as they did in Croatia and Bosnia. More: MPRI, "A Global Provider of Integrated Training and Safety Solutions, 2012, p. 35, www.mpri.com/. Accessed February 20, 2024.

private security companies - PSCs²¹) both at the national (individual countries) and international levels (international organizations: UN, EU²², African Union AU, North Atlantic Treaty Organization - NATO, and various international non-governmental organizations)²³. PSS companies conducted business lobbying for participation in UN peacekeeping missions through the British Association of Private Security Companies (BAPSC²⁴) and the International Stability Operations Association (ISOA²⁵), formerly known as the International Peacekeeping Operations Association (IPOA²⁶), dedicated to providing ethical services to international peacekeeping, humanitarian rescue, stabilization efforts and disaster relief (Brooks, 2012: 11).

In this sense, in recent decades, the private security industry has played an increasingly significant role in post-conflict operations of the UN²⁷, the EU and its member states, and international non-governmental organizations as direct humanitarian actors in multilateral peacekeeping missions²⁸. However, there is no general agreement among states in the world on the use of PSS companies in post-conflict UN missions, given that their normative regulation is regulated differently from country to country, i.e. there is no uniform regulation in states around the world. In multilateral peacekeeping missions, the UN most often entrusts the implementation of tasks to NATO, the EU, the OSCE, the CIS and the OAU, while the UN delegates a smaller number of tasks to the

²¹ The term PSC covers a wide range of services that a company can provide, including both military and non-military support, as well as armed and unarmed security to smaller security companies that provide specific security services, and are specialized in providing military expertise, including combat operations, strategic planning and intelligence Ibidem p. 28.

²² In 2003, EU forces were deployed in the eastern part of Congo – Ituri province, as part of a limited crisis management operation called "Artemis", with a UN mandate, in accordance with UN Security Council Resolution 1484, which authorized the deployment of a 16-member interim multinational force under French command without NATO cooperation. See: *Crisis management in sub-Saharan Africa – the role of the European Union*, Occasional Paper 51, April 2004, ISS, Paris, p. 41. Fernanda, Faria, *Crisis management in sub-Saharan Africa – the role of the European Union*, Occasional Paper no 55, ISS-EU, December, 2004, p.66.

²³ See: UN Global Study on the implementation of the UN Security Council Resolution 1325: *Preventing Conflict, Transforming Justice, Securing the Peace*.

²⁴ More: BAPSC www.bapsc.org.uk

²⁵ More: ISOA: <http://stabiliti-operations.org/indek.php>

²⁶ More: IPOA: www.ipoaonline.org

²⁷ The UN's position as a single universal international organization exempts it from great transparency, accountability, reform and has no competitor in peacekeeping procedures. See: UN Global Study on the implementation of the UN Security Council Resolution 1325: *Preventing Conflict, Transforming Justice, Securing the Peace* (2015), p. 69.

²⁸ The demand for private contractors as business-oriented entities has increased, due to the reduction in the number of military forces in the world since the end of the Cold War and the increasing use of peacekeeping forces around the world. See: Laura A. Dickinson, (2011) *Outsourcing War and Peace: Preserving Public Values in a World of Privatized Foreign Affairs* (New Haven: Yale University Press), p. 11.

private security sector as commercially contracted support to UN peacekeeping activities in various missions, under the effective supervision of the UN Secretary-General.²⁹

Essentially PSS in peacekeeping operations, i.e. stabilization and post-conflict reconstruction operations, contributes to the sustainability of UN peacekeeping operations, and responds to critical situations in a fast, impartial manner and without bureaucracy, where PSS companies implement a wide range of services and activities: combat and operational support, military advice and training, weapons procurement, intelligence collection, security and crime prevention services as well as logistical support (Schneekener, 2006: 23–41).

From the point of view of the direct participation of PSS companies in post-conflict missions, the UN criticizes their individual engagement, due to their occasional violations of human rights and disregard for international law, but they continue to engage them on a contractual basis for their peacekeeping missions, most often within the framework of partnership programs³⁰ and to fill gaps in procurement, as well as for certain security services. Thus, the EU has engaged private security companies to protect the headquarters of EUPOL in Afghanistan, to secure the premises of the EULEX mission in Kosovo and to guard the EUPOL mission in the Democratic Republic of the Congo (DR Congo), etc. When it comes to the direct participation of states in post-conflict peacekeeping missions, they can independently engage private security actors on a commercial-contractual basis, whereby the PSS also gains a certain level of national legitimacy for its activities. Regarding post-conflict missions of various international non-governmental organizations (UNESCO, International Red Cross, WHO, UN High Commissioner for Refugees, World Bank, IMF, etc.), the role of PSS companies is most often personnel safety, protection and deterrence (Messner, 2007: 73).

Given the changing nature of conflicts, the changing role and capacity of the state, the increasing privatization of traditional domains of the state, and especially the new role of non-state actors in multilateral UN operations, adequate and transparent representation of PSS operations in post-conflict missions is essential to support conflict mitigation (Tsifakis, 2012: 17).

From the past practice of contracting the private security sector in various UN stabilization and post-conflict reconstruction missions, certain multiple advantages of PSS

²⁹ The involvement of PSS companies in post-conflict missions in Africa (Sudan, Sierra Leone and Angola) is particularly pronounced (2800 PSS companies), given that the most important problems on the continent are human security and intractable conflicts, which were caused by previous peace failures of some Western countries in the 1990s in Somalia and Rwanda. More: Thomas Jäger and Gerhard Kümmel, (2007) *Private Military and Security Companies: Chances, Problems, Pitfalls and Prospects*, 1st edition (Wiesbaden: VS Verlag für Sozialwissenschaften), p. 28.

³⁰ An example of a partnership program is the US Global Peacekeeping Operations Initiative (GPOI) with the role of PSSs in distributing information, as nodes in the network that is formed when the mission begins. More: state.gov/t/pm/ppa/GPOI.

have been noted: the ability to create rapid response teams; the flexibility to assist organizations and states to improve human security; financial optimality; efficiency; control and accountability; the ability to protect international non-governmental organizations from real threats; the ability to implement affordable security sector reform; the legitimacy of the engaged party (UN, EU or member states); effectiveness of initial peacekeeping and enforcement; geopolitical and political apathy; contracts based on quality, not price, and the same dictate the terms of service delivery; high probability of successful delivery of contracted services; competitiveness of services and greater technological capability, training, and level of innovation than most militaries (Chesterman & Fisher, 2009: 22).

On the other hand, the private security sector is not equally aligned with the international response to conflicts and the problems are particularly evident in conflict countries where the rule of law and democratic governance are weak or where there is widespread armed violence, so PSS is not immune to certain irregularities: PSS companies are there for the money, they have no real interest in maintaining peace; they can be corrupt and paid by the other party in the post-conflict; in transitional or post-conflict states, they can act as an obstacle to peacebuilding, good governance and sustainable development; they can only fulfill the contract and nothing more, for example, they want to prolong the conflict or disaster indefinitely, so that they can continue their activities; they can reduce the number of staff or use less trained staff, in order to reduce costs; they are not morally committed, there is no real loss other than money if they do not implement the activities; they can withdraw; reduced or limited liability of the contractual relationship; lack of a single regulation of conduct, i.e. they do not have a clear international legal status³¹, this sector has the potential to become a force in its own right and are usually not held accountable for their actions; human rights violations and criminal violations for which there has been no accountability; they can be used against weaker governments; they support the rich and those in power; UN companies and PSS as peacekeepers are competition.

Finally, practice indicates that extensive reliance on PSS companies in multilateral peacekeeping operations risks making weak states even weaker in three segments: creating a false picture of the security situation and a proper assessment of security needs; distorting the distribution of security among the population and crowding out the establishment of functional state institutions (Jager & Kummel, 2007: 33).

³¹ International regulation is less successful, particularly due to confusion regarding the general definition of “mercenaries” as private armed security providers. The United States has the most advanced regulation in the field of private security. At the level of self-regulation of private security industry companies, within the framework of the International Peacekeeping Operations Association (IPOA), there is only a code of ethics for the conduct of companies in post-conflict activities of multilateral operations. Also, there is no general agreement in the world on the international engagement of PSS companies. More: Laura A. Dickinson, (2011), *Outsourcing War and Peace: Preserving Public Values in a World of Privatized Foreign Affairs* (New Haven: Yale University Press), p. 45.

CONCLUSION

Given that the global population continues to grow and that global economic, demographic and climate trends are inexorably eroding the traditional balance of power in the international system, it is undeniable that interstate conflicts are likely to increase. In this regard, a number of risks may today influence the trend of increasing interstate conflicts: regional competition encourages unilateral action by states³²; states become polarized along ethnic or religious lines (ethnicity, religion or both become factors of group identification and the basis for political organization)³³; the institutional capacity of state institutions and the rate of economic growth affect the ability of a state to provide equal benefits to its entire population; economic interdependence is growing (state economies are interconnected with each other and with the global economy); an increasing number of states, with modern state-level resources, are developing advanced capabilities that are potentially useful in conflicts³⁴; the constant progress of information and communication technologies and population movements, as transnational factors, require multi-level governance; the erosion of the international order makes it difficult to build consensus and confront global threats;³⁵ increasing climate change causes a decrease in arable land, food and water resources, and population migration (in combination with greater competition for limited natural resources and demographic pressures, there is an overload of state capacity and a lack of resources, which also increases environmental insecurity).

Such risks, on the one hand, include regional instability, high humanitarian needs, mass migration, human trafficking, social inequality and exclusion, demographic change, rapid and unplanned urbanization, exploitation of weak governments, and global economic and other shocks, which are likely to persist in the medium and long term.

³² In the Middle East and North Africa, regional powers are pursuing competing security interests, driven by growing military and economic capabilities. Both South Asia and Southeast Asia continue to grow in economic importance and political significance, but this comes with increased tensions, exacerbated by unresolved historical disputes. More: Denney, L. Mallett, R. & Mazurana, D. (2015). *Economic and Political Causes of Conflict: An Overview and Some Policy Implications*. CRISE, University of Oxford, Working Paper No. 81, February 2015, p. 12.

³³ Extremism and instability in the Middle East and Africa have displaced millions of people, Ibid, p.24.

³⁴ There is increasing access by states and non-state actors to the technologies necessary to produce and use lethal weapons, including nuclear, chemical, biological and radiological weapons or destructive cyber technology. The scale and severity of the threat from serious and organised crime is also increasing, as more services and transactions take place on social media. See: World Bank and United Nations (2017); *Pathways for peace: Inclusive approaches to preventing violent conflict*, International Bank for Reconstruction and Development/The World Bank, p. 48.

³⁵ The global state system is characterized by a hierarchy still dominated by the United States in terms of military and economic power, its central role in international governance, and its position as a supporter and enforcer of international norms. Ibid, p. 51.

On the other hand, the prevention of interstate conflicts requires the search for inclusive solutions such as: dialogue, adapted macroeconomic policies; institutional reform of key state functions, with redistributive policies (reducing inequality); the human and economic cost of interstate conflicts around the world requires increasingly collaborative work; national development actors should provide greater support to national and regional conflict prevention programs³⁶, through flexible and sustained engagement; international conflict prevention agendas (post-Cold War peace projects³⁷) should be integrated into development policies and efforts of states: continuous investment in inclusive and sustainable development of society; systemic addressing of inequality and exclusion in society; transparency of national development strategies and making institutions more inclusive.

In general, analyzing all of the above, several moments clearly dominate: *first*, the complexity of the global security context has led to a change in the drivers of interstate conflicts, as well as a change in the nature of violent conflict due to the changing national security context, *second*, the necessity of the existence of effective international mechanisms for mediating conflicts (the growth of international consensus and norms against the violent change of borders, accompanied by a commensurate growth of more effective international organizations that can implement these norms), together with the credible threat of external intervention, especially for peacekeeping operations authorized by the United Nations³⁸, and *third*, the use of private security companies in the prevention of interstate conflicts must be hybrid (superordinate, well-regulated, monitored, integrated and controlled), where its speed and flexibility are most often used to maximize the effectiveness of establishing peacekeeping missions under the mandate of the UN Security Council.

Therefore, it can be safely said that the best answers lie in fully understanding the advantages and disadvantages of using PSS companies in multilateral UN missions,

³⁶ The 2004 European Neighbourhood Policy, which defines the EU's relations with the 16 closest eastern and southern countries, is aimed at stabilising the region in political, state and security terms, the 2011 EU Conflict Prevention Programme. More: Cameron, F., Balfour, R. (2006) The European neighbourhood policy as a conflict prevention tool. EPC Issue Paper, no. 47, p. 53.

³⁷ The Maastricht Treaty of the EU countries (1992) has the explicit goal of maintaining peace and strengthening international security in accordance with the UN Charter; the EU Summit in Petersburg (1999), when the European Security and Defense Policy was formulated and a project for the development of rapid reaction forces was adopted; the EU Treaty of Nice (2000), regarding the creation of an arrangement with NATO, the so-called Berlin-Plus arrangement; the Treaty establishing the Constitution of the EU (2004), which envisages that the EU will not only be a political and economic union but also a military-defense pact, i.e. with a Common Defense Policy and clauses on mutual assistance in the event of military aggression against one of the member states and action in peacekeeping operations. See: Giovanna Bono, (2006), "The Perils of Conceiving EU Foreign Policy as a Civilizing Force, in IPG 1/2006, p. 155.

³⁸ There will remain crises that require only professional forces to maintain peace or create it if it does not exist, since the UN does not always have the resources to do what is needed to establish or maintain peace. More: Denney, L. Mallett, R. & Mazurana, D. (2015). *Peacebuilding and Service Delivery*. United Nations University Centre for Policy Research, February 2015, p. 33.

as well as knowing the risks and weighing the costs and benefits of each action taken, where eliminating the possible use of PSS for peacekeeping³⁹ is unacceptable.

REFERENCE LIST

Schmid, P.A. (1998). *Thesaurus and Glossary of Early Warning and Conflict Prevention Terms*. Synthesis Foundation.

Cameron, F., Balfour, R. (2006). The European neighbourhood policy as a conflict prevention tool. *EPC Issue Paper*, no. 47.

Carayannis, T. (2018). Rethinking the Politics of Violent Conflict. Social Science Research Council, <https://items.ssrc.org/rethinking-the-politics-of-violent-conflict/>.

CPPAC, Conflict Prevention Tools (2015): Multi-Stakeholder Processes for Conflict Prevention and Peacebuilding: A Manual, November (2015), ENDNOTES.

Crisis management in sub-Saharan Africa- the role of the European Union, *Occasional Paper* 51, April (2004), ISS, Paris.

Denney, L. Mallett, R. & Mazurana, D. (2015). Economic and Political Causes of Conflict: An Overview and Some Policy Implications, CRISE, University of Oxford, *Working Paper* No. 81, February 2015.

Denney, L. Mallett, R. & Mazurana, D. (2015). *Peacebuilding and Service Delivery*, United Nations University Centre for Policy Research, February 2015.

Brooks, D. (2002). Private military service providers: Africa's welcome pariahs. *Guerres D'Afrique*, Laurent Bachelard, Ed., *Nouveaux Mondes*, No 10 - Printemps, Centre De Recherches Entreprises Et Societes.

Faria, F. (2004). Crisis management in sub-Saharan Africa – the role of the European Union, *Occasional Paper* no 55, ISS-EU, December (2004).

Gowan, R. (2012). The United Nations, Regional Organizations and a New Generation of Challenges. Geneva: International Forum for the Challenges of the Peace Operations.

Bono, G. (2006). The Perils of Conceiving EU Foreign Policy as a Civilizing Force, u *IPG* 1/2006.

Haider, H. (2014). *Conflict: Topic Guide* (Chapter 3: Preventing and Managing Violent Conflict), Governance and Social Development Resource Centre.

Bercovitch, J. Kremenyuk, V. and Zartman, I. W. (eds.). (2008). *Handbook of Conflict Resolution*, London: SAGE.

International Alert. (2015). *Building prosperity and peace: Integrating peacebuilding into economic development*, London: International Alert.

Messner, J. (2007) *Ethical Security: The Private Sector in Peace and Stability*, Operations Library.

³⁹ There are no definitive answers when it comes to finding "what uniquely works" in peacekeeping.

Avruch, K. (2009). Culture theory, culture clash, and the practice of conflict resolution, in: Sandole, D.J.D., Byrne, S., Sandole, I. and Senehi, J. (eds.), *Handbook of Conflict Analysis and Resolution*, Routledge, New York.

Krause, K. (2016). From Armed Conflict to Political Violence: Mapping & Explaining Conflict Trends. *Daedalus* Volume 145, Issue 4, <https://doi.org/10.1162/DAED.a.00416>.

Dickinson, L.A. (2011). *Outsourcing War and Peace: Preserving Public Values in a World of Privatized Foreign Affairs* (New Haven: Yale University Press).

Lund, M. S. (2009). Conflict Prevention: Theory in Pursuit of Policy and Practice. in: Bercovitch, Kremenjuk, V. & Zartman, I. W.(eds). *The SAGE Handbook of Conflict Resolution*.

Michael S. Lund (2009): Conflict Prevention: Theory in Pursuit of Policy and Practice, *the Sage Handbook on Conflict Resolution*. London: Sage Publications Ltd.

MPRI. (2011). A Global Provider of Integrated Training and Safety Solutions, www.mpri.com/.

Nakarada, R. & Baljetbo, A. (ur.). (2007). *Uloga posredovanja u međunarodnim sukobima*, Univerzitet u Beogradu – Fakultet političkih nauka i Fundacion Internacional Olof Palme, Beograd.

Peace Research Institute Oslo (PRIO), (2018), *Trends in Armed Conflict, 1946–2017*. PRIO. <https://reliefweb.int/sites/reliefweb.int/files/resources/Dupuy%2C%20Rustad-%20Trends%20in%20Armed%20Conflict%2C%201946%E2%80%932017%2C%20Conflict%20Trends%205-2018.pdf>.

Chesterman, S. & Fisher, A. (eds.) (2009). *Private Security, Public Order: The Outsourcing of Public Services and Its Limits*. Oxford; New York: Oxford University Press.

Fisher, F. (ed.). (2000). *Working With Conflicts-Skills & Strategies for Action*, Zed Books, London.

Tsifakis, N. (2012). Contracting with PVZK. Originally quoted in David Isenberg, "The Devil's Always in the Details," Washington, DC: Huffington Post, July 25.

Jager, T & Kummel, G. (2007). *Private Military and Security Companies: Chances, Problems, Pitfalls and Prospects*, 1. Aufl. ed. (Wiesbaden: VS Verlag für Sozialwissenschaften)

UN Global Study on the implementation of the UN Security Council Resolution 1325: *Preventing Conflict, Transforming Justice, Securing the Peace*, (2015).

United Nations and World Bank Flagship Study; *Sustaining Peace: making Development Work for Prevention of Violent Conflicts*, Concept Note, October 13, (2016).

Uppsala Universitet – Department of Peace and Conflict Research: Definitions, Internet, (2011), <http://www.pcr.uu.se/research/ucdp/definitions/>.

Schneckener, U. (2006). Fragile statehood, armed non-state actors and security governance. in: Bryden, A & Caparini, M. (eds). *Private Actors and Security Governance*, Lit Verlag, Berlin.

Schneckener, U. (2010). Dealing with armed non-state actors in state-and-peace-building: types and strategies. in: Benedek, W. Daase, C. & Van Dyne, P. (eds), *Transnational Terrorism, Organised Crime and Peace-building*, Palgrave, Basingstoke.

Von Einsiedel, S. et al. (2017). *Civil War Trends and the Changing Nature of Armed Conflict*. UNU-CPR. [https://collections.unu.edu/eserv/UNU:6156/Civil war trends UPDATED. Pdf](https://collections.unu.edu/eserv/UNU:6156/Civil_war_trends_UPDATED.Pdf).

Watts, S. (2017). *Understanding Conflict Trends: a Review of the Social Science Literature on the Causes of Conflict*. Rand Corporation. [https://www.rand.org/pubs/research reports/ RR1063z1. html](https://www.rand.org/pubs/research_reports/RR1063z1.html).

World Bank and United Nations (2018). *Pathways to Peace: Inclusive Approaches to Preventing Violent Conflict*. [https://open knowledge. World bank org / bit-stream /handle/ 10986/28337/211162mm](https://openknowledge.worldbank.org/bitstream/handle/10986/28337/211162mm).

World Bank Group Flagship Report, International Bank for Reconstruction and Development, 2023/ The World Bank 1818 H Street NW, Washington, DC 20433, www.worldbank.org, ISSN: 0163-5085 ISBN: 978-1-4648-1941-4.

BAPSC www.bapsc.org.uk.

ISOA: <http://stabiliti-operations.org/indek.php>.

IPOA: www.ipoaonline.org.

<http://www.un.org/en/charter-united-nations>.

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309 Cm 9161 NSS SD Review](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review).

www.un.org.

ww.mpri.com.

*Miriam Ugulava*¹

ISLAMIC FUNDAMENTALISM AND ITS ROLE IN POLITICIZING RELIGION

Abstract

Fundamentalism conjures images of those uncompromising religious factions that trace everything back to its beginnings and provide perspectives and interpretations of modern problems grounded in earlier ethical and intellectual traditions. Global religious fundamentalism gave rise to radicalism; Muslim radicals can be found in Afghanistan, Egypt, Bangladesh, Iraq, Nigeria, Syria, and Yemen; Christian radicals can be found in the Philippines and United States and the Jewish radicals can be found in New York and Palestine, while Sikh and Hindu radicals can be found in India, and Buddhist radicals can be found in Myanmar. The history of Islamic fundamentalism predates Islam itself. Fundamentalism is a sociocultural movement that resisted social changes. Islamic fundamentalism is not only a problem in the Muslim world. It poses a threat to the world order and people's well-being. Islamic fundamentalism has long been a significant challenge to international security. The topic is very relevant and interesting in its meaning; it actually represents the everyday life of the world. When we talk about religion, what comes to mind is people united under a particular faith, whose spirit is usually connected with peace, love and humanity. However, at the same time, no matter how surprising, the same concept is associated with war, intolerance, bloodshed and various types of violence. Therefore, a legitimate question can be asked: How can one and the same religion fill one person with goodness, and call another for evil and violence? Religion is built on philosophical-ideological foundations, but it also echoes cultural and ethical norms established in society. Why and how was the Islamic religion connected with terror? It is important to consider who is to blame and what the real threats to the state and social security of the world are.

Keywords: *Islam, civilization, fundamentalism, politics, terrorism.*

ISLAMIC FUNDAMENTALISM

If we look at the etymological meaning of the word – in the language, fundamentalism is taken from the verb "origin" of a thing; the basis on which it is based. This is not the concept of fundamentalism only in Arabic, but in other languages as well. This means that fundamentalism in all languages means going back to the beginning (Hussein, 2020).

¹ Georgian Technical University, Faculty of Law and International Relations, Miriam.ugulava77@gmail.com

Historically, the word fundamentalism is not known in Arabic, not even any religious group knows this term, which strictly adheres to its dogmas. The meaning of the concept of fundamentalism, as we know it today, was not long established in the Arabic language. The term appeared in the West only in the last three decades of the 20th century, and then it was transferred to Arabic (Glend, 1999).

So, fundamentalism is defined in the most known languages and it means going back to the beginning. Fundamentalism has become synonymous with violence and extremism. In western political discourse, the term fundamentalism is often used to refer to religious extremism, usually in the "orthodox" or "ultra-orthodox" form (Al-Jasur, 2004). All forms of rational interpretation are opposed by Islamic fundamentalism; it tries to adapt the divine text to the present time and place (Hero, 1997).

The concept of fundamentalism now has a political and intellectual connotation associated with negativity, especially after the emergence of Islamic radical groups that use Islamic slogans to guide their politics. Their politics is as follows: chaos, violence, terror. Many Islamist terrorist organizations have a fundamentalist character and their ideology is radical, such as Al Qaeda, Hamas and ISIS. A fundamentalist view considers western civilization as an enemy (Sen Nag, 2017).

The origin of Islamic fundamentalism is related to two historical periods. The first was the Abbasid period. The second is the modern era, the period of the establishment of the Muslim Brotherhood in Egypt. The second period is considered a continuation of the first.

Islam's core beliefs include that the Quran contains revelations from God (Allah) to Muhammad, who is the prophet, and that Allah is the source of all truth. The enunciated legal system, political framework, code of ethics, as well as code of religious and civil activities make up the Sharia (Rabie, 2021).

The Quran and Sunna are the two main sources used by Muslim fundamentalists (groups, individuals, and preachers) who view Islam as a temporal religion and seek to apply Sharia to politics and social interactions. The Quran and the Sunna are acknowledged as the primary sources of law, morality, values, visions, and perspectives in all of these groups' literature and by their academics. Nothing in the Quran and Sunna can be contradicted or violated by human law. According to them, the Quran should serve as the foundation for the correct Islamic community establishment in both public and private spheres, serving as a guide for all of its major and minor life decisions (Arkoun, 1996).

Fundamentalists believe that the Quran is the source of unchanging divine truth, which must be adhered to rigorously and literally, regardless of the passage of time or location. Other holy texts, including the book of Muslims, have been perverted and contain no truth; only the Quran is a genuine "divine document". It is the sole piece of divine writing that hasn't been changed or twisted (Al-Badawi, 2002).

The story of the origin of Islam is connected with a real person and it is connected with the name of Muhammad Ibn Abdullah (570-632). Due to his way of life and field of activity, Muhammad traveled often and possessed considerable knowledge about Judaism and Christianity (Amina, 2002). Muhammad is considered the founder of Islam, he actually laid the foundations of a new religion. As a result of the beginnings of this religion and its historical review, it is established that Islam was originally created as a tool of political rule. And Muhammad made great changes in the political, religious and social processes of his time (Nasr, 2003)

Before Islam, the Arabs lived as separate tribes, which were often at odds with each other, and the only way to resolve disputes between them was through bloody confrontation. Muhammad offered them a completely new reality, a new society, where God-Allah stood at the head, and he was in the role of his messenger. According to his narration, Muhammad's actions were sanctioned by Allah himself. With this idea Muhammad took upon himself all the functions of a ruler (Gelovani & Sanikidze, 2009).

After the above-mentioned sermons and the sounding of the idea, Muhammad was confronted by the family aristocracy. Muhammad's situation in Mecca became unbearable and he left Mecca and moved to Yasrib, which is denoted by the Arabic term "Hijra". The Hijra is the basis of the Muslim calendar. Yasrib was called the city of the prophet, Madinah (Medina), after the exile of Muhammad (Gelovani & Sanikidze, 2009). Muhammad's role in Medina differs from his work in Mecca, as he now appears as a far-sighted politician, since his original goal was to create a political union in Medina. In the city of Medina, Muhammad underwent a complete transformation, just like the Quran (Nasr, 2003). It is interesting that Islam in Mecca condemned all forms of violence in religion.

Muhammad gradually becomes the ruler of Medina and uses all the tools and leverage of a ruler. From this period, the foundations of the politicization of Islam appear clearly, when Muhammad tries to unite the Arabs politically, using Islam and in its name.

Here we can see the origin of the ancient Islamic state, when the community of Medina, under the leadership of Muhammad, was governed based on the collection of laws, which was the first "constitution" of the Islamic State for them. It is significant that the above-mentioned community association formed in Medina and the main goal of its expansion was "Jihad" (war), which primarily meant an armed confrontation against the Mecca unbelievers. Subsequently, Muhammad actively used Jihad to advance his policies. After the conquest of Mecca, the Arabian Peninsula was Islamized and the process of forming a Muslim state began (Quran, ayat 9: 29).

Muhammad is considered the founder of Islam; he actually laid the foundations of a new religion. As a result of the beginnings of this religion and its historical overview, it is established that Islam was originally created as a tool of political rule. The duality of Muhammad and the Quran makes Islam a very flexible and accommodating religion. It turns out that actually everything depends on the political position of

a Muslim in a particular country (Shboul, 2020).

Peoples of the Islamic world have experienced a period of awakening during the past 200 years, which is typified by the following major fundamentalist movements:

1. Muslim Brotherhood in Egypt,
2. Khomeinism in Iran,
3. Amal and Hezbollah in Lebanon,
4. Hamas in Palestine,
5. Sanusi in Libya, Mahdiyya in Sudan, Ahmadiyya in India, and Wahhabi in Saudi Arabia. (Rabie, 2021).

There are different definitions of traditional Islam. A relatively modern definition was formed after the collapse of the Soviet Union. Over time, an understanding of traditional Islam was formed to prevent the importation of political Islam. And traditional Islam itself meant an understanding that is not dictated by political narratives and does not interfere with political activity (Abilov, 2021).

Religious fundamentalism differs sharply from traditional Islam, because it completely rejects the possibility of a secular state. According to fundamentalists, the state organization should be based on the principles of Islamic law. Islamic fundamentalism preaches a return to ancient beginnings, such as adopting the lifestyle of Muhammad's time. According to their opinion, Islam should be the means of internal and external management of the state.

The most important content values identified by Islamic fundamentalists are as follows (Khosravi, 2006):

1. The comprehensiveness of Islam so that it encompasses all aspects of human life;
2. Islamic fundamentalism depends on politics;
3. The idea of going back to the beginning;
4. Formation of the Islamic State;
5. The pragmatism of Islamic fundamentalism and its militaristic nature.

For Islamic fundamentalists, Islam is not just a religion; it is a political, social and economic system and it is a civilization that extends to all times, countries and places (Shboul, 2020). The goal of the sociopolitical movement known as fundamentalism is to restore the Islamic society of the past, but its idea of this past is still hazy, misinterpreted, and susceptible to a variety of occasionally divergent theological viewpoints. Members of this movement are united by their similar religious beliefs despite their differences in politics, as well as their memories of a terrible experience of injustice (Norton, 1985). "Islamic fundamentalism and radicalism is not a monolithic entity", claims Augustus Norton. It is a complex blend of movements, parties, and societies with a wide range of objectives, plans, and driving forces.

Radicalism is a mindset shaped by shifting social and political conditions, whereas fundamentalism is a deeply held ideology founded on specific religious ideas and traditions. Violence has always been justified as a means to an end by the marginalized but ideologically devoted forces throughout history (Rabie, 2021).

For most believers, fundamentalism is an ideology with an adequate model of social and political change, which is a source of communal identity and national pride. "Fundamentalism is the protest and resistance to any form of power that is not guided by divine scripture" (Marranci, 2009).

POLITICAL ISLAM

The widest definition of political Islam is the collection of contemporary political groups, intellectual fads, and state-mandated initiatives aimed at granting Islam a position of authority in politics. The Muslim Brotherhood movement, which was started in 1928 in Isma'iliyya, Egypt, and has branches associated and semiaffiliated throughout the Muslim world and nations where Muslims reside, is the main source of organized political Islam (Andrew, 2015).

Hassan al-Banna is a founder of the Muslim Brotherhood organization. Al-Banna believed that jihad was the duty of all Muslims and everyone had to be ready for war at any time. Over time, the popularity of the Muslim Brothers grew and it was manifested in the fact that the brothers become the main and strong opposition of the government. This was due to the fact that they had support and popularity in the lower layers of society and trade unions (Ghattas, 2001).

Political Islam seems to have varied aspects in different historical processes, since it has been the topic of considerable discussion in the media, political and academic circles (Abdullah, 2022).

Even before, scholars like Muti'i (1926) and al-Khidr Husayn ('Imara, 1989) responded with greater force to the 1918 fall of the Ottoman Caliphate and to the secularist manifesto of al-Azhar scholar 'Abd al-Raziq (1925), *Islam and the Foundations of Government* (Ali, 2005), and other nineteenth-century figures like Jamal al-Din al-Afghani (Andrew, 2015).

Generally speaking, political Islam is associated with the right of the political spectrum. However, it would be incorrect to regard it as a single movement or philosophy. First, Islamists have different traditions about religious knowledge and authority. Some Islamists maintain that Muslims who are not technically schooled can still understand Islam's political message while rejecting the conventional sources and practices of premodern orthodox religion. Crucially, "interpretive modernism" of this kind does not always imply political or moral liberalism (Andrew, 2015). Like many left-leaning or even liberal Islamists, the leading theorists of the more conservative, utopian school

of political Islam were self-taught rather than classically trained experts (Andrew, 2015).

However, it is incorrect to say that this rejection of conventional intellectual authority represents all of Islamism (Zaman, 2002). Many Western intellectuals and political Islamists share the belief that Islam has given rise to a political force in modernity because Islam is fundamentally political. The fact that Islam never historically developed the institutional separation between a corporate "church" and a corporate "state", out of which functional secularism could evolve, the fact that Islam is closely linked to the public enforcement of a religious doctrine, and the fact that the Prophet Muhammad was a political and military leader who established Islam as a political entity, are common points of contention for this viewpoint (Roy, 1994).

The phenomenon referred to as political Islam is based on the modern revival of religion in both public and private spheres (Esposito, 2000). On the one hand, a lot of Muslims have started to observe more strictly the tenets of their faith, such as prayer, fasting, clothing, and family. Conversely, Islam has made a comeback as a counter to the ideas that secular ideologies like nationalism, capitalism, and socialism are deemed to be ineffective (Esposito, 2000).

Political and social activism is now informed by Islamic symbols, discourse, actors, and organizations, which have become sources of legitimacy and mobilization. Islam has been invoked by the governments of Afghanistan, Iran, Egypt, Malaysia, Libya, Saudi Arabia, Morocco, Pakistan, and Sudan in an effort to bolster their legitimacy and garner support from the general public for various initiatives and policies (Esposito, 2000).

Islamic movements range from moderate to extremist in terms of their religious and political views. The Muslim Brotherhoods in Egypt, Sudan, and Jordan; Jamaat-i-Islami in South Asia; the Refah party in Turkey; the Islamic Salvation Front in Algeria; al Nahda in Tunisia and others have been among the more well-known (Esposito, 2000). Modernization has been seen as a bad thing that replaces religion and cultural identity, akin to neocolonialism (Esposito, 2000).

Governments, decision-makers and analysts have faced political and intellectual challenges from Political Islam regarding foreign policy, pluralism, democratization, modernization and development, leadership and ideology, as well as modernization (Esposito, 2000). Political Islam is seen by many countries as a danger to both their internal and global security. This claim is supported by bombs and killings that have occurred in North America, Europe and the Middle East. Still, there are unanswered questions, such as: Should radical fundamentalists be held responsible for societal issues? (Esposito, 2000).

Political Islam evolves over time. It is interesting the social role of political Islam, which is a form of expression of one or another social group. Usually, Islamists have support from the representatives of the middle class, and they have special support from the social class which is against any progress (Gavrilin, 2010). Political Islam is not a specific ideology, although it can be tentatively divided into two opposing positions: Islamic radicalism and

Islamic liberalism. All Islamist radicals are fundamentalists who interpret Islam very narrowly and interpret the Quran literally to fulfill their own purposes (Gavrilin, 2010).

As for liberal Islamism, it is loyal to democratic values, recognizes human and citizen rights, and pluralism as values consistent with Islam (Gavrilin, 2010).

While modernization theory dissuaded mainstream social science from examining Islam's political impact prior to the Iranian revolution of 1979, scholars of Islamism consistently argue that the ideology is fundamentally intertwined with the issue of modernity, and thus warrants examination in conjunction with other antiliberal, reactionary, or populist modern ideologies (Lerner, 1958).

Islamists actively use modern technologies to carry out their actions. Therefore, they are very well informed about both technological advances and other modern issues. The modern Muslim world faces challenges related to local, traditional, and global relationships as well as modernization. Muslim societies struggle with issues including corruption, economic growth, efficient government, and democratic mobilization against autocracies or powerful elites (Pandya, 2009).

When recognizing the contribution of religious thought to political development in the Muslim world, it is crucial to define this link precisely. It is also critical to understand that the fusion of politics and religion is a worldwide trend. In Muslim civilizations perhaps religion and its cultural impacts are more important than in any other region of the world. But religion also matters because it advances certain social and political objectives, sometimes in secret. Islamism encompasses a wide range of political and ideological stances. Anti-Western attitude is a defining characteristic of certain movements, reformist political organization of others, and revolutionary mobilization of still others. Some will use violence in practice, some will support it philosophically, and still others will only put up with it (Pandya, 2009).

It is critical to examine and distinguish between the political, religious, and cultural when political goals are expressed in terms of culture and religion. First, we may separate the parts of religious discourse that are really political discussions from those that are related to faith. It should also be evident that Islam appeals in different and diverse ways to identity, custom, ritual, and faith as well as to ideals regarding how society should be ordered (Pandya, 2009).

Every element has an impact on public life and the political process. Only then will one be able to recognize the unique and different ways in which Islam resolves social, political, or economic disputes, calms psychological concerns brought on by modernization or the startlingly quick speed of change, or acts as a catalyst for spiritual development (Pandya, 2009).

We should also keep in mind that practically every aspect of Muslim religion and culture, such as the rise in religiosity, the focus on outward markers of religious identity, the advancement of political agendas derived from religious sources of knowledge, and

the feeling of cultural rebirth, has an equivalent in non-Muslim cultures (Pandya, 2009).

Regretfully, there will be those on both sides who support the other's darkest concerns. In actuality, a large number of Muslims harbor strong animosity toward the West and think that terrorism is a kind of jihad due more to religious fervor than theological instruction. As they genuinely believe that Islam justifies and rationalizes hatred and violence against non-Muslims, their counterparts in the West are all too eager to tolerate drastic (and ineffective) actions against the Muslim world (Pandya, 2009).

Today, terrorism has become closely intertwined with Islamic fundamentalism, and these concepts have become almost synonymous for many. This is not surprising, since people have watched the "heroic deeds" of Islamic terrorist organizations almost daily for years, although it has been established that terrorists in many cases are not necessarily strict followers of their religion.

On October 7, 2023, the group Hamas launched a military attack in the direction of the Israeli territory. This group is considered a terrorist organization by many states, and their main idea is Muslim-fundamentalist. Hamas has become a very dangerous hybrid organization. It no longer fights with the old methods, on the contrary, it has turned into a highly effective military armed force that has elements of both a terrorist organization and a military unit (Emanuilov, 2011).

Based on all of the above, it can be said that Hamas as a terrorist group initiated a very large military conflict in the Middle East, and their main goal is to is the liberation of Palestine from a non-Muslim nation as well as their subsequent seizure of powerful control.

Israel's ambassador to the United Nations, Gilad Erdan, during his speech at the United Nations, said that the President of Iran, Ebrahim Rais, met with the leaders of Hamas, and the meetings were held in Syria and Lebanon. He also noted that Iran was trying to coordinate terrorist armies, its proxies in the region. Their main goal is to destroy Israel using the nuclear umbrella that Iran will provide to the terrorists (Najdi, 2023).

Hamas won the 2006 Palestinian parliamentary elections and as a result established control over the Gaza Strip. The forces of Yasser Arafat's successor, President Mahmoud Abbas, were driven out. The international community stopped aid to the territory controlled by Hamas, because they consider Hamas a terrorist organization (Toameh, 2014).

ISIS (Islamic State of Iraq and Syria) is a group of Sunni jihadists; it originated in 1999 in Jordan. It is a Salafi terrorist organization and its "active" establishment can be considered the year 2004, when its name was "Al-Qaeda in Iraq". From that period it joined Al-Qaeda and became a kind of its branch (Jasko, Kruglanski, 2018). The end of the Islamic State begins in 2017, although the atrocities committed by them are indelible; according to the data of the New York Times, they have killed 1,200 people outside of Iraq and Syria (Younish et al., 2016). Also, according to CNN data, 143 terrorist acts were carried out by the Islamic State in 29 countries and 2043 people were killed (Lister et al., 2018).

On March 22, 2024 at 6:00 p.m. in Russia armed persons attacked the citizens in the concert hall in Krasnogorsk. It was written in the New York Times that the Afghan branch of the Islamic State might be behind the terrorist attack; they took revenge on Russia for Chechnya, Afghanistan and Syria (Troianovski, Mazeeva, 2024).

It is thought that there are complex relationships between terrorist groups and large countries, companies or centers of power. Various allegations have been brought forward that some terrorist acts were financed and initiated by groups that benefit from them.

Regardless of its origin, the most important problem caused by Islamic fundamentalism is Islamophobia. This is a common mistake that people who are not affiliated with Islam perceive the religion of Islam or all Muslims by associating them with terrorism. Accordingly, many Muslims who have nothing to do with terrorism or extremism are excluded and exposed to various prejudices in the countries they live.

The issue of jihad is fundamental to Islam's conception of itself as well as the Western world's concomitant concern that it justifies violence against the West. Islam is a distinct religion since it emphasizes mobilization. Though on a spiritual level, the founding society placed a strong focus on organizing for social action and opposing archaic traditions and ethnic divisions. The oppositional stance itself is likely to cause non-Muslim concerns and feelings of confrontation, whether or not this actually makes Islam's relationships with others confrontational. The sense of conflict will be strongest when the appeal is made to a sense of justice against unfair and dictatorial political and economic systems, and when jihad is mentioned.

CONCLUSION

Islam is distinctly different, own, individual and it took its place among the monotheistic religions, which at the time was characterized by considerable specificity; essentially, it differed ideologically from other monotheistic religions. Islam, which is the firstborn of Prophet Muhammad and his revelations became the unifying force for the Arabian tribes, which stood out for each other and there was no force that could unite them under one banner to conversion form of a powerful political force of Arab tribes.

From time immemorial, Islam represented not only a union of believers, but also a political society consisting of them. That is why the management of the state should be carried out by religious laws, Sharia, which would remain unchanged in relation to time and space, since it was the word of God. Islam has become a necessary prerequisite for the functioning of the state. That is why the highest teacher of the Muslim community was a person who accommodated the function of religious development of the community and conversion to it. The subject of the dispute is the management of the government, since the highest authority belonged to Allah.

The main goal of Islamists is confrontation with the West and re-Islamization, although they do not ignore western technical achievements on this path; on the contrary, they wanted to achieve their goal by using this technical development. They believed that the main law maker was God. Therefore, they reject the separation of public authorities in any form and especially law-making. Thus, Islamism became a real struggle to usurp power in a revolutionary way, to unite the secular and clerical authorities, and for a spiritual leader to rule the country according to Islamic rules.

It can be safely said that Muhammad created a religion that was also political in nature, combining its main political goals with religious considerations and began the struggle to create a new state. Despite the religious preaching, political processes accompanied him. For Muhammad as a person it was clear that without certain political processes the Islamic doctrine could not win. Thus, Islam was distinguished from its germ in connection with politics.

The scientific world was not initially interested in the phenomenon of political Islam, which emerged at the beginning of the 20th century within the context of the Islamic awakening. This occurred as a result of Islamism's association with Islam's all-inclusiveness, which unites all the three domains: political, religious, and socioeconomic. In contrast to ideas, values, and cultural norms specifically associated with or derived from Islam as a religion, the adjective "Islamic" is frequently used to describe what makes Muslim societies and customs unique (for which the adjective "Muslim" is more appropriate).

It is incorrect to refer to terms like "fundamentalist", "radical", "extremist", "militant" or "moderate" as nouns; rather, they are adjectives. It is critical to define their eligibility. When we discuss the reading of religious texts, criticisms of social structures, political institutions, or the tendency toward violence, are we talking about radicalism, extremism, or moderation? What does the term "reflexive use of the term militant" actually mean? This is a phrase that has been used recently in secular discourse to characterize unwavering, principled, or purist approaches to political practice, particularly in Western trade union movements and European political parties. How did this come to be used for groups that are a combination of terrorist, insurgent, or radical ideologies? Furthermore, why does "fundamentalism" in religion – defined as a return to the foundations or to the original texts – necessarily entail a certain perspective on social justice, political activity, or political ideology?

In the early stages of Islam, the foundation of the unity of religion and politics was laid. In fact, from the day of its origin, Islam turned into a religious doctrine on the one hand and a political program on the other. From the day of its origin, Muslims and their prophets fought a political struggle.

Over the centuries, there was one principle in the explanation of the nature of government by Islam, which was that all and all power in the world belonged to Allah; according to the principles of Islam, one group of people on Earth is given the right to rule over other groups of people.

REFERENCE LIST

- Arkoun, M. (1996). *Islamic Thought: Scientific Reading* (Translated by Hashem Saleh, 2nd ed., p. 145). Beirut: Arab Development Center.
- Al-Badawi, J. (2002). *The Green Sword: A Study in Contemporary Islamic Fundamentalism* (pp. 21 and 22). Cairo: Dar Qaba for Printing and Publishing.
- Al-Jasur, N. M. (2004). *Encyclopedia of Political Science* (p. 64). Amman: Majdalawi Printing and Publishing House.
- Adil, H. A. (2002). *Muhammad, the Messenger of Islam: His Life & Prophecy*. Washington, D.C.: Islamic Supreme Council of America.
- Abdullah ÖZÇELİK, 2022.
- Andrew F. March (2015). *Political Islam: Theory*.
- Bedford, S. Ceyhun Mahmudlu, C & Abilov, B. M. (2021). Protecting Nation, State and Government: 'Traditional Islam' in Azerbaijan, *Europe-Asia Studies*, 73:4, pp. 691-712, DOI: 10.1080/09668136.2021.1899136
- Emanuilov, R. & Yashlavsky, A. (2011). *Terror in the name of faith: religion and political violence*, Boston: Academic Studies Press, <https://doi.org/10.1515/9781618110596>
- Esposito, J. L. (2000). *Political Islam and the west*. Spring 2000/JFQ Forum.
- Gavrilin, E. (2010). *General characteristics of political Islam*.
- Glend, M. El-S. (1999). *Fundamentalism and Dialogue with the Other* (p. 10). Cairo: Dar Qabaa for Printing and Publishing.
- Ghattas, Kim, "Profile: Egypt's Muslim Brotherhood". *BBC* (9 February 2001).
- Gelovani N., Sanikidze, G. (2009). *Islam (Religion, History, Civilization)*. Tbilisi, University Publishing House.
- Hero, L. (1997). *Islamic Fundamentalism in the Modern Age*, Translated by Abdel Hamid Fahmy Al-Gammal Cairo: Egyptian Book Authority.
- Hussein, I. A. S. (n.d.). (2020). *Fundamentalism and Other Fundamentalisms*, Beirut: Dar Al-Kutub Al-Alamia.
- Katarzyna Jasko, Arie W. Kruglanski, Ahmad Saiful Rijal Bin Hasan, Rohan Gunaratna (2018). *ISIS: Its History, Ideology, and Psychology*.
- Khosravi, G.R. (2006). A Preface to Islamic Fundamentalism. *Strategic Studies Quarterly*, Vol. 9, No. 31.
- Lister, T. Sanchez, R. Bixler, M. Sean O'Key, Hogenmiller, M. and Tawfeeq, M. (2018) *CNN - 'ISIS goes global*.
- Lerner D. 1958. *The Passing of Traditional Society*. London: Collier-Macmillan.
- Marranci, G. (2009). *Understanding Muslim Identity, Rethinking Fundamentalism* https://dl.uswr.ac.ir/bitstream/Hannan/130542/1/Gabriele_Marranci_Understanding_Muslim_Identity_Rethinking_Fundamentalism__2009.pdf
- Najdi, Y. (2023). *Benjamin Restle, Israel-Hamas war: What is Iran's role?*
- Nasr, S. H. (2003). *Islam Religion, History, and Civilization*.

- Norton, A. (1985). Islamic fundamentalism and Islamic radicalism: hearings before the Subcommittee on Europe and the Middle East of the Committee on Foreign Affairs.
- Pandya, A. (2009). *Islam and Politics, Renewal and Resistance in the Muslim World. Quran*, ayat 9:29.
- Rabie, M. (2021) *The Rise of Islamic Fundamentalism*. Roy O. (1994) *The Failure of Political Islam*. Cambridge, MA: Harvard University Press.
- Shboul, H. (2020) Discussing Islamic Fundamentalism and Its Role in Politicizing Religion. *Open Journal of Political Science*, 10.
- Sen Nag, O. (2017). What Is Religious Fundamentalism? *World Atlas*.
- Troianovski, A. and Mazaeva M. (2024), *The New York Times*.
- Yourish K., Watkis, D., Giratikanon T., and Lee C.J. (2016) *The New York Times*, How Many People Have Been Killed in ISIS Attacks Around the World.
- Zaman M.Q. 2002. *The Ulama in Contemporary Islam: Custodians of Change*. Princeton, NJ: Princeton Univ. Press.

Vladan Borović¹
Stefana Matović²

ADVANCED SYSTEMS FOR REMOTE DETERMINATION OF THE POSITION OF MILITARY UNITS IN SPACE

Abstract

The main feature of existing systems for remote determination of the position of objects in space is the extremely high cost of use, the possibility of interference with GPS signals, frequent imprecise data and errors, as well as dependence on a third party - the owner of satellite systems and technologies. As a result, most field operations could not be covered by these systems for many years. The chance of potential, new systems, detection by video camera traversal, increases with possible multi-purpose use. The aim of this paper is to describe and introduce new technologies for detecting the position of objects in space, adopting a strategy and plan, taking actions and analyzing the adopted strategy. Today, the most common applications of such systems are in tennis, football and cricket, then for police and military purposes, as well as in manufacturing, industrial branches of society such as the automotive industry. These are analog systems, with the same technology and multipurpose use. The assumption is that systems for remote determination of the position of objects in 3D space based on triangulation of video signals with 3 or more HD video cameras and appropriate software provide precise and unambiguous detection, results and positional data of objects. This scientific paper describes a unique approach to the detection and tracking of moving objects, with a description of the newly designed authoring system, a review of existing solutions, experiments and analysis. Experimental and statistical scientific methods were used with the application of comparative analysis. The authors described the developed, original 3D system used in determining the position of objects in space. The authors described and tested an advanced system for detection and tracking of objects, proved the efficiency of the new system and proposed its introduction into operational use.

Keywords: *Object Detection, 3D Position, Software, Triangulation.*

¹ Ministry of Internal Affairs, Belgrade, Serbia, vladan.borovic@mup.gov.rs

² Research Associate, Geographical Institute "Jovan Cvijić" SANU, Belgrade, Serbia

INTRODUCTION TO TECHNOLOGY

Systems for tracking moving objects in space

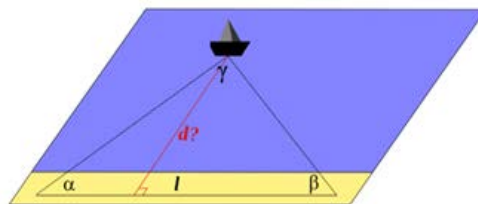
The idea of designing such a system from the very beginning implied a lot of time spent studying the functioning of each part of the system, starting from mathematical problems to technical finesse. From the very beginning of the development of the object tracking system, the authors of the paper were faced with a large number of requirements, problems and unknowns. Everything indicated that information about previous, similar systems was kept secret. The most important existing systems will be described in this chapter.

The basic mathematical principle for determining the position of objects is the well-known principle of triangulation in geometry. The public is most often familiar with this term in the field of telecommunications, when finding and locating mobile phones and their users. This principle consists of a series of tested and optimized mathematical functions that have proven their correctness in practical field testing. Triangulation is the process of determining the location of a point by measuring the angles to it from known points on opposite sides of a fixed baseline. This point can thus become the third fixed point of a triangle with one known side and two known angles. The method is most widely used in trigonometry and geometry. Triangulation can also refer to the precise surveying of systems of large triangles, called triangulation networks. It is a continuation of the work of the Dutch mathematician Willebrord Snell in 1615 and 1617, who showed how it was possible to locate a point using the angles formed by three known points, a problem called resection. Such triangulation methods for surveying and surveying large areas of the Earth, large geographical areas, were used until the introduction of the first Global Navigation Satellite Systems in the early 1980s (Triangulation Surveying, 2018).

If we define mathematical terms more precisely, triangulation is a method for determining the coordinates and distance from a desired point by calculating the length of one side of a triangle, with known values of the angles and sides of the triangle formed by that point and two other known points, the so-called reference points, and using the sine of the angle (Borović et al., 2019).

Optical 3D measurement systems also use this principle to determine the spatial dimensions and geometry of the observed object (Borović et al., 2019).

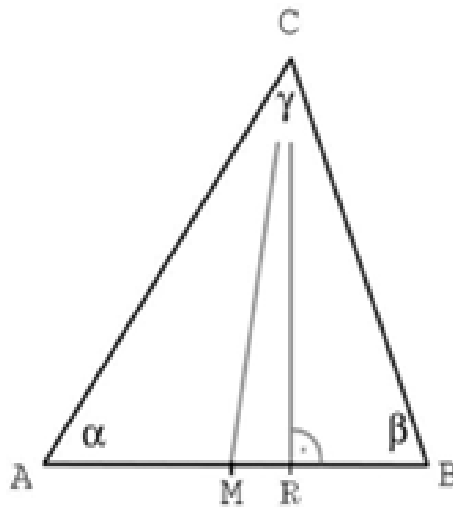
Figure 1. Application of the triangulation method to determine the position of a ship (Triangulation_(surveying), 2018)



Figures 1 and 2 show solutions to an example of determining the position and the mathematical functions from the described principle of triangulation for determining the position of a ship relative to the shore.

In Figure 1, l represents the distance between two known reference points, and α , β and γ are the angles between the sides of the triangle formed by the three points, practically α and β are the angles between the shore and the ship at two different reference points. Of course, the unknown quantity is the distance d of the ship from the shore, which we can determine, if the above-mentioned quantities are known, by applying the sine of the angle. In addition to the distance, the exact coordinates of the point where the ship is located can also be determined, which is of extreme importance.

Figure 2. *Triangulation method*



Where are: A, B – reference points; M, R – control, measurement points, C – the desired point where the ship is located.

Tracking objects using the GPS system.

According to UNOOSA (United Nations Office for Outer Space Affairs), 8,378 objects have been launched into space so far in history. Currently, 4,994 are still in orbit – although 7 of them are in orbit around celestial bodies other than Earth – which means that there are 4,987 satellites moving above our heads every day (Pixalytics consultancy company, 2019).

These satellites make up a functional network of GPS satellites. Initially, 24 satellites were needed to set up the system. They, of course, also provide basic information about the weather, network status and orbital positions (Pixalytics consultancy company, 2019).

Each satellite continuously broadcasts signals containing three basic types of information:

1. *Almanac*

A set of data that tells the GPS receiver where each satellite should be in the sky during a 24-hour period. All satellites transmit this signal, so the GPS receiver has information about all orbits in the system if it can locate, i.e. capture, only one satellite.

2. *Pseudorandom code*

It represents the so-called "name and surname" of the satellite, i.e. the designation of the satellite that sends the signal and can be read by the GPS receiver and is 1023 bits in size, transmitted every millisecond.

3. *Ephemeris*

Ephemeris data contains:

- information about the status of the satellite ("healthy" or "unhealthy"), which means whether it can, at a given moment, be used for navigation or not,
- the date and very precise time of sending the signal, which is the most important data for determining the position.

Each satellite carries up to four cesium and rubidium atomic clocks, which are very precise and expensive, and are periodically corrected and adjusted from a ground station in Colorado.

A GPS receiver is a device that calculates its position based on distance measurements from three or more GPS satellites. Each satellite transmits a microwave sequence of radio signals that is known to the receiver. As the receiver receives this signal, it is able to determine the time that elapses between the transmission of the radio signal from the satellite and its reception at its position. The distance of the receiver from the satellite is calculated based on this time, since the radio signal travels at a known speed. The signal also carries information about the current position of the satellite from which it is transmitted. If the distance of the receiver from the satellite and the position of the satellite are known, it is known that the receiver is located somewhere on a sphere of a certain dimension with the satellite at its center, as in Figure 4. Since the positions of the three satellites and the distance of the receiver from each of them are known, the position of the receiver can be determined by the process of trilateration, i.e. triangulation. Trilateration is based on the fact that three spheres intersect at most two points (one of which usually makes no sense).

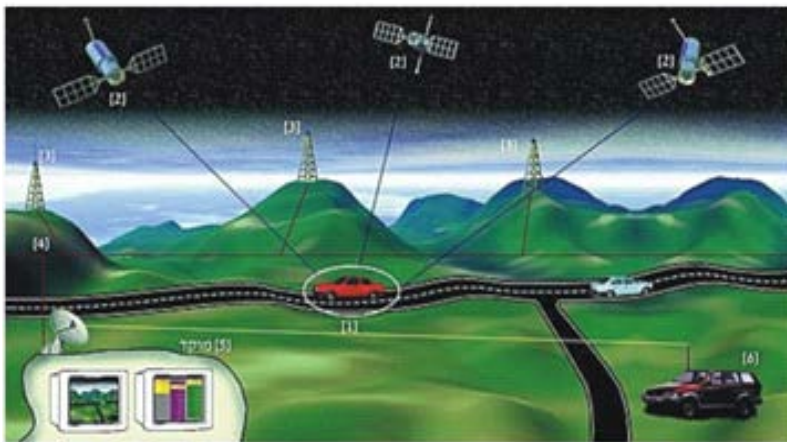
This principle of operation implies that the clocks on all satellites and on the receiver are fully synchronized in order to accurately measure the time difference between the known sequence of signals from the satellite and the receiver. The satellites contain atomic clocks. However, the receiver has a much less precise clock, a crystal oscillator. The lack of precision is solved by introducing distance measurements from another satellite. The clock on the receiver introduces the same time and space error when calculating the distance from all four satellites. It can be calculated by how much the clock

needs to be corrected in order for the four spheres to intersect at the same point. In this way, the clock on the receiver is continuously corrected. One of the applications of GPS is very precise time calculation and clock synchronization (Borović et al., 2018).

When a GPS receiver receives a signal, it compares the difference between the moment the signal was sent from the satellite and the current time. Based on this difference, which is actually the time the signal travels from the satellite to the receiver, the distance to the satellite is determined. By processing signals from at least three satellites, using the triangulation method, it is possible to precisely determine the position of the receiver on the Earth. Precisely, three satellites are sufficient to determine two-dimensional coordinates, i.e. latitude and longitude. In order to determine the third dimension in space, the altitude at which the object is located, we need signals from at least four satellites, at any time when determining the position of objects in space. The precision of determining the position of objects in space is high, even up to a few centimeters (Bajaj, Ranaweera, 2002).

When all the temporal data are known, the speed of movement of objects, the distance traveled, the rate of climb and descent, and the time to a specific target can be calculated, which have multipurpose significance in numerous areas of public, commercial, civil, and military-police applications.

Figure 3. *Determining the GPS position of an object using the triangulation method*



Source: Borović, V. (2006). *GPS/GPRS sistem za daljinsko praćenje – telematika*, Stručni projekat za licencu, Savez inženjera Srbije, p. 52.

Figures 3 and 4 show methods for determining the position of objects in space using satellite signals from the GPS system and ground stations. It is clearly seen that the desired object on Earth is located in the intersection of three spheres formed by the satellites in the triangulation process.

Figure 4. *GPS triangulation method – the tracked object is in the intersection of a sphere*



Source: Borović, V. (2006).

Tracking objects using cameras

The most well-known use of video camera-based systems in the public today is in the detection and tracking of people and objects, suspicious things and events, as well as recording all movement paths of the observed subject under surveillance and the surveillance area. These applications are most often in the police and the military. Also, due to the increased risk of global pandemics, video camera systems are used in remote temperature measurement of people.

As shown in Figure 5 and Figure 6, the possibility of technically satisfactory tracking of moving objects using publicly available algorithms for pattern recognition, position and motion detection is realistically achievable in commercial systems and with smaller financial investments and outlays (Kirillov, 2007).

As can be clearly seen in Figure 5, the red rectangles around the detected moving objects mark the detection of movement in the video, more precisely the slight movement of people, while in Figure 6 it is easy to see the detection of the position and movement of vehicles on the road from the video using a software application.

At first glance, it is clear that, as shown in the pictures, the main disadvantages of these systems are the low and insufficient speed of position detection, slow video processing, insufficient calculation accuracy, and above all the low number of frames per second, which is a technical characteristic of this video equipment. The aforementioned disadvantages are primarily driven by the entire algorithm for tracking moving objects, the improvement of which, through a new approach and optimization, through the speed and accuracy of tracking moving objects in space, was carried out by the authors of this paper in their new advanced tracking system in sports and police-military fields.

Figure 5. Simple software application for monitoring



Source: Borović et al. (2019). Supervisory system for physical objects spatial location detection. *Physica A: Statistical Mechanics and its Applications*, Volume 521, pp: 781-795

Figure 6. Detection and tracking of vehicle movement on the road



Source: Borović et al. (2019).

Figures 5 and 6 show, under optimal daytime conditions, the application of algorithms for shape recognition, detection of position and movement of objects, with very low optimization of video footage, low speed and accuracy of position detection in space. Otherwise, the aforementioned images show that the number of frames per second is only 2.07 fps, which is extremely low, absolutely insufficient for more precise calculations of fast moving objects, and insufficiently precise detected shapes of individual tracking objects.

Analysis and review of the state of existing systems

The first system, which was also the basis for the design and construction of the advanced, modern system that is the subject of this paper, is described in the scientific paper (Borović et al., 2019). This system included and applied the methods of the time, primarily software with libraries for detecting objects and their positions in space.

Until 2018, the available software applications for pattern recognition and object position detection on video cameras were significantly different from today's, with worse features and poorer performance. Also, the authors then applied their own algorithm, which has since been changed and improved.

The technology described in this paper has been applied in many areas, with a great possibility of expanding its application. Numerous spheres of interest have been using similar systems for many years in the chain of making referee and automatic strategic decisions by calculating the necessary and difficult-to-calculate information. They are slowly taking on a very important role in decision-making. It is important to list some of the most important applications by field of work: (Lović, Rabiei, Matović, 2022; Babović, Matović, Lović, Radovanović, 2016).

- Systems applied in sports,
- Systems applied in the automotive industry,
- Systems applied for police and military purposes.

In terms of police and military use, one of the most well-known systems for detecting position in space using GPS systems and video cameras is the Northrop Grumman E-2D Advanced Hawkeye (AHE), an American all-weather aircraft designed for early warning and alerting, shown in Figure 7. It was developed in the late 1950s and early 1960s in the United States. The last, fourth major modern version, bears the designation E-2D, and dates from 2010 (Northrop Grumman, 2017).

In addition, starting from the 1960s, new technology and techniques of aerial surveillance were introduced, which are now represented in many countries around the world.

Figure 7. *Appearance of the E-2D Advanced Hawkeye (AHE) aircraft*



A sophisticated system of radars, cameras and various sensors remotely detects people, technical equipment and machinery and determines their position in space. At the same time, a three-dimensional terrain model is precisely determined and calculated. Since the system is functional at very high altitudes, almost imperceptible operational work is possible even from considerable distances. Also, there are a larger number of these aircraft in use, more than fifty, therefore the calculation results are even more precise (Northrop Grumman, 2017).

Since the use of drones and other unmanned aerial vehicles is very widespread and popular today, these systems are installed and used on general and wide-use aircraft, such as the Ehang GHOSTDRONE 2.0 Aerial Plus (Android Version) unmanned aircraft in the form of a so-called drone, a small helicopter equipped with 4KHD sports cameras with technical characteristics of 1080p@120fps (pixels and frames per second), shown in Figure 8. The aircraft is controlled by remote controls via a mobile phone or other smartphone. The applications on the phone contain a precise map of the terrain and show the points that the aircraft flies over (EhangGHOSTDRONE 2019). Of course, although the main purpose is remote surveillance from a height, it can be equipped with fast sports cameras for determining the position of objects in space using triangulation.

Figure 8. *Surveillance mini-drone equipped with a sports camera*



The remote control and surveillance system for video areas is shown in Figure 9, which clearly shows that it is possible to reliably guide the aircraft to monitor a given area of entertainment events, e.g. a sports field, where the use of multiple aircraft results in more precise calculations that can be used to detect the position of objects in space. Images from the video cameras can be displayed on an Android device, as well as the results of the calculations. A graphical simulation of the trajectory can be displayed on the screen of multiple mobile phones simultaneously.

Figure 9. *Android software for remote control of the aircraft (EhangGHOSTDRONE 2019)*



Today, systems are used with great success in the automotive industry, primarily computerized systems for adjusting the camber and adjusting the direction of the wheels of cars and other vehicles. These systems are based on the principle of triangulation, hence the technical principle often mentioned in the name. There are usually two cameras in the system. Their distance and angles are known in advance, so it is possible to apply the principle of triangulation and certain mathematical calculations and then calculate the angles and distances in the entire system. Each sensor has a reference system consisting of two CCD cameras. Stereo cameras are used to determine the position of the axis of rotation of the wheels. The following images show some examples of practically applied computer systems (NUSSBAUM group, 2017):

Figure 10. *Computerized camber adjustment system with four high-resolution cameras*



ADVANCED MOBILE OBJECT TRACKING SYSTEM

In the past five years, there has been significant progress and development of software applications for pattern recognition and object position detection on video cameras, which, with the application of new algorithms for tracking moving objects in space, greatly increase the accuracy and quality of the entire process. The use of a new software framework and libraries for position detection and object recognition applied in a new concept and setting of a new algorithm leads to significant progress and improvement in the performance of the tracking system (Borović et al., 2019).

The advanced tracking system has the following units, independent subsystems, each of which has certain roles:

- Signal acquisition subsystem,
- Subsystem for advanced detection of objects and positions in three-dimensional space,
- System for 3D simulation, animation and graphical display of calculation results.

The first subsystem, an independent unit, consists of a mandatory system of video cameras and technical equipment that monitors and records a sports match or action. It is also possible to record other areas with different tasks. This system, at the same time, collects signals in real time on a certain, larger number of computers according to the following model:

1 camera = 1 associated computer.

The second unit consists of a subsystem that, based on the image from the cameras (on-line) or based on the recording (off-line), determines the position and simulates the trajectory of the observed object in space, e.g. a vehicle in the field. The system consists of software developed in the Microsoft programming environment, with the program code written in MS Visual Studio C++ and C# 98, 2010, 2013 programming languages. Testing and practical implementation were done for the image-based object detection and tracking system. It will also be described. Otherwise, the basis of the system for detecting and tracking moving objects in space is made up of new, current and improved publicly available mathematical algorithms with the application of mathematical principles (Borović et al., 2019).

The third unit consists of a system that, based on the calculation of the object's trajectory in space, performs a graphic simulation of 3D animation in an attractive and visually appealing manner. A software application for precise, photorealistic 3D visual display is the basis of this independent unit.

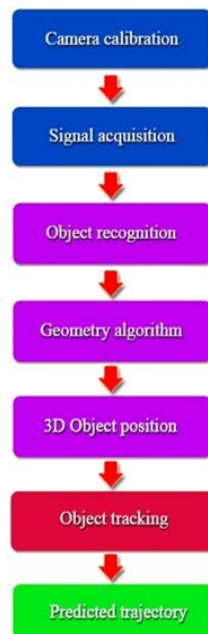
During the design of the new, advanced system for tracking moving objects, with all its subsystems and units, numerous technical consultations were held with renowned experts in the fields of electrical engineering, mathematics and applied programming. Also, during practical testing, a great contribution was made by workers employed on sports fields, primarily in the field of tennis.

In each image sent from each camera, the system identifies a group of pixels that corresponds to the image of the object being observed, i.e. whose movement is being tracked. After recognizing the object's shape, the 3D position of the object for each frame per second recorded by the video camera signal acquisition is calculated by comparing the position of at least two physically separate video cameras at the same time. The sequence of frames, with the prediction, creates a record of the path the object has traveled. Then, using this calculated data and the predicted path of the object, it calculates where the path intersects the observed terrain. The system compares the position of contact with the ground with predefined terrain dimensions.

As a final result, this system creates a graphical simulation, photorealistic 3D animation and a graphical image of the object's trajectory and the observed area. Its purpose can be in a large number of areas with a variety of topics. Reproduction is in almost real time (Borović et al., 2019).

Figure 11. shows, in the form of an algorithm, the entire process of the Advanced System for Tracking Moving Objects. As in the state space, the entire system goes through various stages - from collecting the necessary data to the final product, the solution, i.e. the predicted trajectory of the observed object. Experimentally correctly selected stage settings, from video camera settings to the selection of algorithms for recognizing objects in the image and detecting motion, with mathematical calculations and optimizations, lead to accurate, reliable and credible tracking results.

Figure 11. *The working process of the Advanced System*



Source: Borović et al. (2019).

TESTING AND EXPERIMENTAL RESULTS

Testing a new algorithm for moving object detection

The main advantage and difference compared to the detection algorithms in AForge.NET, as shown in practical testing, is that the new selective algorithm provides positions and processed, much simpler and clearer images, for further path calculation. Instead of searching for objects in the entire camera image, with a large number of colors, it immediately detects the only green object on a black background. The next step, prediction, is therefore faster, simpler and requires less memory and processor resources.

Table 1 shows the experimental test results, calculated position X and calculated position Y (in pixels), detection of ball movement and contact with the court line, in images from the video camera in the plane of that line. In the 18th frame, the ball contacted the court, which is documented in the image from the video camera as shown in Figure 12.

Table 1. *Comparative analysis of two algorithmsa*

Frame (s)	Object (No.)	<i>AForge.NET v2.2.5 (2013.)</i>		<i>New selective algorithm</i>	
		Position X (pixel)	Position Y (pixel)	Position X (pixel)	Position Y (pixel)
11. 0.03	1	16	80	16	79
12. 0.06	1	48	72	49	72
13. 0.09	1	92	67	93	67
14. 0.12	1	136	64	136	63
15. 0.15	1	180	52	180	50
16. 0.18	1	216	34	217	34
17. 0.21	1	254	16	254	16
18. 0.24	1	288	2	288	0
19. 0.27	1	300	29	299	27

The obtained experimental results show the following:

- * The moment of contact of the ball with the surface is marked in red, frame 18, height 0. The new algorithm gives more precise and reliable results. The version of the algorithms from AForge.NET incorrectly detects the height of the ball;
- * The possibility of an error in the detection of the older version of the algorithm is significantly higher than the new one;

The experimental results from Table 1 are finally shown as the final result of the monitoring and electronic decision-making system in the system for 3D simulation, animation and graphical display of results in Figure 12.

Figure 12. Analysis results shown in 3D simulation



a) Frame 17 same for both algorithms, b) Frame 18 in red, position detection error for the old algorithm and c) Result of electronic refereeing

It is clearly seen in Figure 12, from the OpenGL 3D animation, that in the 17th frame identical coordinates were detected, but in the next one, due to the incorrect calculation of the position using the version of the algorithms from AForge.NET, a shift occurred in the 18th frame, which ultimately leads to the wrong decision that the ball is out of bounds (in red). The new algorithm of the author of this paper gives the correct results (in black), which is confirmed by comparing the actual video recording and the moment of contact of the ball with the field in Figure 13.

Figure 13. Real image from video camera – clearly visible contact of the ball with the line



Based on the results obtained, it can be concluded that:

* The new ball detection algorithm provides better results in tracking moving objects in tennis and the possibility of error in electronic decisions of the older version of the algorithm is significantly higher than in the new one.

Testing AForge.NET

At the same time, a third test was performed, in addition to the previous test, the results of which are given in Table 2, a video recording was made and analyzed on the other video camera, in HD resolution, 60 fps, with identical camera settings.

Table 2. *Dependence of the number of detected objects on the resolution*

	<i>Ultra HD</i>	<i>HD</i>
Frame (s)	Object (No.)	Object (No.)
1. 0.016	5	3
2. 0.032	6	4
3. 0.048	7	5
4. 0.064	7	5
5. 0.080	8	6
6. 0.096	8	7
7. 0.112	8	7
8. 0.128	10	8
9. 0.144	10	9
10. 0.160	10	10
11. 0.176	10	9

The experimental results obtained show a higher number of detected objects in images when using the Ultra HD video mode compared to HD on video cameras. The large number of detected objects can be confusing, but this is a consequence of the very high resolution of the videos made or in real time for the video cameras used.

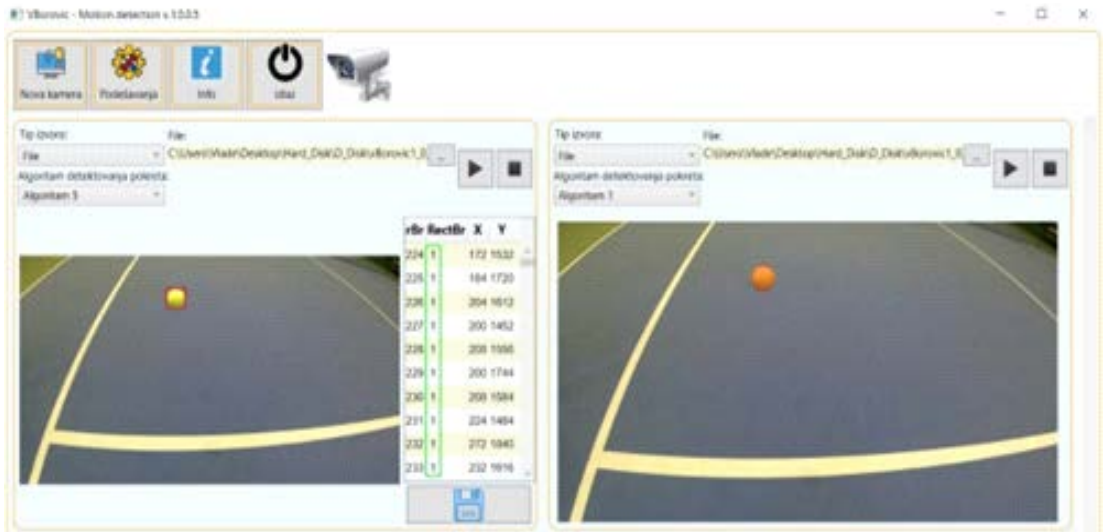
Based on the numerical data obtained through experimental testing, it can be concluded that:

- * In the Ultra HD video mode of the camera, it is possible to detect a larger number of objects than in the HD mode in each image taken from the video camera, which increases the accuracy and reliability of the detection of moving objects in the tracking system;
- * At the same time, the Ultra HD detection mode is significantly more sensitive and susceptible to external influences, error factors such as changes in the intensity and shades of light, small insects and slow shadows, so additional optimizations and filters are required when detecting and tracking balls.

This means that better results are achieved in Ultra HD, a higher and higher quality resolution of the video camera, but more careful adjustment of the algorithms and more detailed processing of each image collected from the cameras is necessary.

The fourth experiment: as a separate test, a video recording was made and analyzed on a video camera, in Full HD resolution, at a speed of 30 fps, The results are shown in Figure 14.

Figure 14. *Ball detection in the software application*



In Figure 14, the number of detected objects per frame is marked in green, as can be seen – one ball per frame. By properly selecting and adjusting the color filter and functions, the green surroundings of the field, similar to the ball, did not negatively affect the detection of the object in the images. Algorithms 5 and 1 are shown in real work side by side (the coordinates are extracted as an example from the recorded file from the disk). In the figure on the left, Algorithm 5 marks the detected ball with a red border rectangle, while on the right, in Algorithm 1, the detection of the ball is shown with a slightly transparent red circle over the tracking object itself.

Based on the visual-graphic results obtained from this detection experiment in difficult conditions, when we have a surrounding area of similar color as the object being tracked, it can be concluded that:

- * By choosing the proposed program framework, video camera and resolution, correct object detection results are achieved with the correct use and adjustment of built-in spatial functions, adequate filters and the use of the author's precise 3D graphic simulation.

CONCLUSION

The use of advanced systems for remote positioning and tracking of mobile military and police objects and units, based on a system of video cameras, software and the mathematical principle of triangulation, introduces a new dimension in timely threat detection, creating the correct strategy and analyzing the situation on the ground, in 3D space. The authors of this paper described existing systems, proposed a new, more efficient algorithm for object detection in the newly designed system, and experimentally proved the effectiveness of using such systems in real-world situations.

The paper experimentally describes and proves that the proposed system provides excellent results in detecting and tracking all types of objects in the field, regardless of the size of the tracked object. The precision of the technology and multifunctionality provide a tactical advantage to security units in operational actions. Its use for military purposes is particularly significant, due to the reduced possibility of interference with detection in space, recognition of the type and purpose of detected objects at a greater distance, analysis of the military situation and creation of an appropriate strategy. Tracking a larger number of moving objects at the same time gives a new dimension to the field execution of military and security tasks.

REFERENCE LIST

Babović (Matović), S., Lović Obradović, S., Radovanović, M. (2016), Foreign Direct Investments in Serbia as a Form of Cross-border Cooperation, *Forum geografic*, Volume XV, Issue 2, pp: 189-194. DOI: 10.5775/fg.2067-4635.2016.231.d,

Bajaj, R. , Ranaweera, S.L. ; Agrawal, D.P., *GPS: Location-tracking technology*, *IEEE Computer Society*; France Telecom R&D, SanFrancisco, CA, USA (2002).

Borović, V. Spalević, P. Jović, S. Jerković, D. Drasute, D. Rančić, D. (2018) Hail suppression activities using TETRA-based sensor network, *Sensor Review*, Emerald Publishing Limited, 39(2), DOI: 10.1108/SR-02-2018-0029, 171-177.

Borović, V. Spalević, P. Čisar, P. Rančić, D. Jović, S. (2019), Supervisory system for physical objects spatial location detection, *Physica A: Statistical Mechanics and its Applications*, DOI: 10.1016/j.physa.2019.01.023 Volume 521, pp:781-795

Borović, V. (2006). *GPS/GPRS sistem za daljinsko praćenje – telematika*, Savez inženjera Srbije, Stručni projekat za licencu, Beograd, pp. 52.

EhangGHOSTDRONE 2.0 AerialPlus. (2019, avgust) <http://www.bestdroneswithcameras.com/ehang-ghost-aerial-plus-drone-android-version/>

Kirillov, A. *Motion Detection Algorithms*. (2007, mart) <http://www.codeproject.com/Articles/10248/Motion-Detection-Algorithms>

Lović Obradović, S., Rabiei-Dastjerdi, H., Matović, S. Identifying spatiotemporal variability of traffic accident mortality. Evidence from the City of Belgrade, Serbia,

Central European Journal of Geography and Sustainable Development (2022), Volume 4, Issue 2, pp: 78-93. DOI:10.47246/CEJGSD.2022.4.2.5

Northrop Grumman E-2D Advanced Hawkeye letelica (2017, avgust). https://en.wikipedia.org/wiki/Northrop_Grumman_E2_Hawkeye#E2D_Advanced_Hawkeye

NUSSBAUM group. *Colour Coded Triangulation*. (2017, maj) <http://www.nussbaum-group.de/italian/business-units/attrezzatura-perofficina/assetti/roboligner/funzioni/wheel-alignment-function.html>

Pixalytics consultancy company. *How many satellites orbiting the Earth in 2019?* <https://www.pixalytics.com/satellites-orbiting-earth-2019/> (2019, 16. januar)

Triangulation_(surveying) [https://en.wikipedia.org/wiki/Triangulation_\(surveying\)](https://en.wikipedia.org/wiki/Triangulation_(surveying)) (2018, decembar)

Triangulation Surveying - Definition, Principle, Advantages and Applications <https://testbook.com/civil-engineering/triangulation-survey> (2019)

Dragan Randelović¹

CYBER SECURITY AS NON-MILITARY SECURITY RISK IN THE INFORMATION SOCIETY

Abstract

In today's society, the use of e-services provided by the Internet is not a privilege of individuals and society, but a reality of globalization and the era of information and communication technologies. Internet technology today represents a common framework of other technologies essential for the development of human society, but also a basic communication tool for solving a wide range of security risks of a dominantly global society, which after the era of the Cold War and the dominant geopolitical and military security risks took on a much wider range of non-military risks, starting from social, health and economic, technological to cultural. Unfortunately, with all the benefits that the Internet provides to users, there is also a "dark" side of the Internet associated with threats on the network that are the basis of non-military security risks in society. Computer security incidents are a frequent occurrence in modern times, and the rapid development of technology and computer science has enabled the development of new methods of attacking and endangering computer systems and networks. Security threats are numerous and diverse, and in order to limit the actions of malicious attackers, it is necessary to establish a procedure for solving security incidents, which has become an important part of information technology. The subject of research of this paper is related to the suppression of Internet crime, specifically the analysis of the place and role of Internet centers for complaints in that process, which as organizations for receiving and helping to resolve complaints about work on the Internet are closely related to organizations that are responsible for receiving, reviewing and responding to reports of security incidents; they can provide services to the government, corporations, educational institutions, but also to private clients and their duty is to provide assistance, protection and security of critical parts of the Internet.

Keywords: *non-military security risk, Internet, cyber security, Internet complaint centers, computer security incident response teams.*

INTRODUCTION

The traditional concept of security in society in the second half of the 20th century was based on the Cold War (Aggestam & Hyde-Price, 2000) and a dominantly military security risk framed by a wide range of security threats to traditional states,

¹ Faculty of Diplomacy and Security, Belgrade, Serbia, dragan.randjelović@fdb.edu.rs

individuals and societies. New forms of nationalism and ethnic conflicts, mass migrations, environmental hazards, resource conflicts, pandemics, transnational terrorism, but also the rapid development of information, biological, chemical, nuclear and other technologies today at the beginning of the 21st century represent a challenge to the conventional approach to understanding threats. This wide spectrum of non-military risks is characterized by overcoming the borders of nation states and interconnectedness through the process of globalization of humanity.

In such a globalized environment, the challenge of maintaining security is not limited to traditional foreign policy and military means, ie geopolitics and military power, but depends on a wider spectrum of social, economic, environmental and other issues (Tuchman, 1989). The framework for all these challenges and issues in such a global information society is Internet computer technology, which enables information as a basic resource to drive the further development of society through the necessary knowledge of individuals. Bearing that in mind, the Internet and cyber security have a special role and importance as a non-military security challenge in this stage of the development of human society, although their role is undeniably great when it comes to military challenges as well. In this overview paper, in which due to the limited scope, we will not deal with the detailed statistical processing of the presented data, the subject is Internet complaint centers and their role through connection with Internet incident response centers, which are directly connected to the appropriate agencies and judicial authorities in charge of law enforcement; thus in the synergistic work of prevention, action and reaction, using Internet complaint centers as the first in that chain, they ensure greater cyber security.

Since the appearance of the first computer in the middle of the last century, until today, there has been an enormous increase in their use. It can be said that today computers have found their application in all areas of people's life and work, in which at the beginning of the 21st century the use of artificial intelligence is a general trend (Varghese et al., 2022; Randelović. et al., 2022; Randelović, 2022; Aleksić et al., 2023). With the development of information technologies, the Internet has become one of the most powerful and widely available communication media on the planet. Using its services in today's modern society is not a privilege of individuals but a reality of globalization and the era of information and communication technologies. Fast, easy and simple access to the Internet expands the possibilities of every person to ensure a better life and facilitate all the necessary communication, which also applies to all kinds of institutional organization of individuals in society.

Knowing that important data is transmitted via the Internet, every user must be aware of the possibility of its misuse. Misuse of confidential data and computer security incidents are frequent occurrences of the modern age. The rapid development of technologies with the aim of creating something useful for humans has enabled the development of new methods of attacking and compromising computer systems and networks.

By providing an adequate system of active protection through work on prevention, as well as reactively and legally adequate treatment of that danger, it is reduced, but not eliminated, so constant updating of the mentioned three types of activities is necessary. The goal of this paper is to practically show that the role of Internet complaint centers in this sense has a special importance in prevention, bearing in mind the role that the data collected there have in the prediction of unwanted incidents as well as the already mentioned trend of increasing implementation of artificial intelligence and machine learning for both offensive and defensive purposes (Velasco, 2022; Ciancaglini, et al., 2020).

1.1. Types of security risks on the Internet

(Brar & Kumar, 2018)

First of all, it is known that there are many different taxonomies of Internet attacks and threats. For example depending on the type of crime committed, internet crime is divided into (Sajid, 2020):

- Political (hacking, cyber warfare, espionage, terrorism, etc.)
- Economic (hacking, cyber espionage, internet fraud, etc.)
- Production and distribution of illegal content (pedophilia, sects, etc.)
- Manipulation of prohibited goods (drugs, weapons, human organs, etc.)
- Violations of privacy (spam, phishing, email monitoring, etc.).

There is also another division that was made based on the method, i.e. the source of origin, into:

- Malware-based attacks (Viruses, worms, and Trojans, Ransomware attacks, Botnets and command-and-control (C&C) attacks, Rootkits and backdoors)
- Web-based attacks (Cross-site scripting (XSS), SQL injection, Cross-site request forgery (CSRF), Phishing and social engineering)
- Attacks targeting operating systems (Buffer overflow attacks, Privilege escalation attacks, Kernel-level attacks, Zero-day exploits)
- Wireless and mobile attacks (Wi-Fi eavesdropping and spoofing, Mobile malware, SMS phishing (smishing), Bluetooth attacks)
- Insider attacks (Unauthorized access, Data theft or exfiltration, Sabotage)
- Physical attacks (Physical theft of devices or assets, Tampering with hardware)
- Social engineering (Phishing, vishing, smishing, Pretexting and impersonation, etc.)
- Network-based attacks (Rapid, 2019) (Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks (Babić et al., 2021), Man-in-the-middle (MITM) attacks, Network scanning etc.)

1.2. The biggest cyber attacks in history

For the sake of a better understanding of the topic discussed in the paper, we will give a brief insight into some of the major cyber attacks in the history of the last 50 years (Babu A, 2023), from which in this paper we will single out the ten largest according to the criteria of their importance and the lessons that can be learned from them (Stewart, 2024):

- The Melissa Virus (1999)

It is one of the earliest known cyber-attacks in the world. Programmer Smith hacked an AOL-American online service provider account and used it to publish a file on the Internet that promised free access to paid adult websites. By downloading the document, he got rid of the virus on their computers.

- NASA cyber attack (1999)

The NASA cyber attack was a breach and subsequent shutdown of NASA key computers for about 21 days.

- Cyber attack in Estonia (2007)

In Estonia, around 58 Estonian websites including websites of government official groups, media and banks were taken offline. DDoS attack overloaded Estonian servers.

- Attack on PlayStation Network (2011)

Hackers stole 77 million PlayStation and Sony online user accounts with their bank card details. The problem lasted for 24 days and the estimated damage was 1-2 billion dollars.

- Adobe Cyber Attack (2013)

At Adobe, 38 million user accounts and Photoshop were hacked by a cyber attack.

- Yahoo Breach (2013 and 2014)

Yahoo's 2013 and 2014 breaches were two of the largest data breaches in history. It affected all 3 billion Yahoo user accounts and was not discovered until 2016. The 2014 hack was carried out by Russian hackers by sending a phishing email to a Yahoo employee.

- VannaCri Ransomware (2017)

VannaCri ransomware infected over 230,000 computers in over 150 countries in May 2017. VannaCri exploited a security vulnerability in the Microsoft Windows operating system called EternalBlue. The malware was spread via phishing emails, and once a computer is infected, it encrypts the files inside and locks the system until payment is made.

- Marriott Hotel Data Breach (2018 and 2022)

A Marriott hotel has revealed it was hit by a massive database breach that exposed the personal information of around 5.2 million guests. The data breach that compromised all guest data was caused by a social engineering attack on a Marriott employee.

- MOVEit (2023)

Progress Software has demonstrated a zero-day vulnerability in its MOVEit file transfer software. The transfer allowed attackers to gain access to MOVEit servers and steal the user data of 60 million people – and this number continues to grow.

1.3. Legal regulation of Internet crime in the world and in the Republic of Serbia (Darijević, 2021)

The legal regulation of computer crime in the world dates back to the second half of the 1980s, when in 1973 a regulation recognizing criminal legal protection against computer crime (Swedish Data Act, amended in 1982) was passed in Sweden, in which the criminal offense of "unauthorized program access" is provided for in Article 21. From then until today, the United Nations, and each of the countries of the world, as well as the European Union, have changed their criminal laws and enacted a number of their legal regulations in connection with this matter. The most significant documents in this regard are certainly the UN Convention on Transnational Organized Crime (the so-called Palermo Convention) from 2000, which our country ratified in 2001, as well as the Council of Europe Convention on High-Technological Crime from 2001 and the Additional Protocol to the Convention on High-Technological Crime from 2003, as well as a series of acts adopted in the years after that in the European Union, such as: Directive of the European Parliament on the fight against sexual abuse, sexual exploitation and child pornography 2011/92EU, Directive 2013/40/EU of the European Parliament on attacks on information systems and replacement of EU Council Framework Decision 2005/222/JHA, Security Agenda of the European Union for the period from 2015 to 2020, Cyber Security Strategy of the European Union from 2013, IOCTA (Internet Organized Crime Threat Assessment, 2017).

Based on and in accordance with confirmed conventions and directives, criminal offenses and sanctions for offenses in the field of Internet crime are regulated in the Republic of Serbia by:

- The Criminal Code of the Republic of Serbia (CPC),
- The Law on the Organization and Competence of State Bodies for the Fight against High-Tech Crime in the Republic of Serbia,
- The Law on the Organization of Courts,
- The Law on Electronic Communications,
- The Law on Information Security, which regulates measures to protect against security risks in information and communication systems, the responsibility of legal entities when managing and using information and communication systems, and determines the competent authorities for the implementation of protection measures and monitoring their correct application in practice.

There are other regulations that regulate this area on different grounds, such as the Law on Ratification of the WIPO Copyright Treaty (Službeni list SRJ, 13/2002), the Law on the Information System of the Republic of Serbia (Službeni glasnik RS, 12/1996), etc. In order for the provision of domestic and international legal assistance to victims of this type of crime to be carried out, certain human behavior must be punishable in the criminal-legal sense, i.e. prescribed by the provisions of the criminal legislation of the given country.

2. Internet centers for complaints

In every country in the world, organizations dealing with security incidents responsible for providing support, information exchange, cooperation with the government and international partners in the field of cybercrime are CERT organizations (Computer Emergency Response Team) or CSIRT (Computer Security Incident Response Team) (Nedeljković et al., 2017). Hierarchically, there are national CERTs in most countries, which is also the case in the Republic of Serbia, which unite the work of other CERTs in the country that deal with the same tasks at a lower level within the organizations and institutions whose Internet security they deal with. There are also supranational CERTs that deal with the subject matter at the level of several countries, such as the CERT of the Republic of Turkey, TR-CERT, a member of the OIC-CERT (Organization of Islamic Cooperation's CERT). CERT provides incident management services such as on-site incident response, support, incident analysis, and others such as warning, training, etc; they can be classified into three categories:

- Reactive services, which are performed based on events or requests
- Proactive services to assist in the preparation and protection of a possibly attacked system
- Services related to security quality; the most common are employee training.

Today, when security threats are numerous and varied, the speed of detection and resolution of problems depends on how much damage the attacked party will suffer. Timely, constant and systematic collection of data on attacks that have occurred, on possible and ongoing incidents on the Internet, is of great importance for the quality work of CERT and the existence and operation of Internet centers for complaints in this sense has a significant role both for victims of Internet crime and for agencies in charge of prevention and prosecution of perpetrators (Randjelović D. & Carević B, 2012). The existence of these centers in the world is logically closely connected with the IT and general development of certain countries in the world, and slowly but surely they are becoming a necessity in each of them.

In this paper, we will deal with the world's most famous and largest complaint centers, namely IC3, which operates in the most developed country in the world - the United States of America and as such covers the whole world, and to a lesser extent due to the natural reasons of the territorial affiliation of the Republic of Serbia to Europe, we will also deal with the European center EC3, and we will only mention that there are such centers in other continents of the world in all developed countries such as, for example, China Internet Network Information Center (CNNIC) in China and Australian Cybercrime Online Reporting Network (ACORN) in Australia. In the Republic of Serbia, such centers are not yet sufficiently developed, although the Center for Safe Internet - Net Patrol works as a non-governmental and CyberCrimeResearch Share (CCRS) thinktank organization, for example. which deal with complaints about the operation of the Internet. Also, the national CERT and the CERT Academic Network of Serbia enable the reporting of incidents on their websites.

2.1 The Internet Crime Complaint Center (IC3)

For victims of Internet crime, primarily in the United States, but also around the world, IC3 is a practical and easy-to-use reporting mechanism that alerts the authorities that there is a suspicion that a crime has been committed. IC3 receives complaints related to Internet crime, considers them, and then makes a report that it forwards to the competent authorities or agencies, and they are the ones who, as necessary, conduct an investigation. IC3 cooperates with the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). The FBI's mission is to protect the United States from criminal intelligence threats and to enforce criminal law within the United States. The role of NW3C is to provide training and investigative support to agencies and organizations involved in the prevention, investigation and prosecution of high-tech crime without investigative powers.

As a center for receiving complaints related to Internet crime, IC3 was established in 2000. Today, in its twenty-fifth year of operation, when Internet crime is a global problem and when technological knowledge is increasingly being used for criminal purposes, IC3 continues to inform the public, provide services and advice on Internet fraud.

Complaints submitted to IC3 refer to all illegal activities on the Internet. The complainant can be a person who is a victim of fraud or a third party. When submitting a complaint, the applicant fills out a form as shown in Figure 1 in which the necessary information is requested.

Figure 1. Initial layout of the complaint submission form (IC3)



The image shows a screenshot of the IC3 complaint submission form. At the top left is the IC3 logo, a globe with a blue 'C'. To the right of the logo is the text 'Internet Crime Complaint Center'. Below the logo and text is a yellow box with the text 'Please Print Name and Address (see example)'. The main form area is titled 'New Internet Submission' and contains several sections with input fields and dropdown menus. The sections include: 'Case Details' with fields for 'Case Number', 'Title', and 'Case Description'; 'Reporting Party' with fields for 'Name', 'Address', 'City', 'State', and 'Zip'; 'Reporting Party Contact Information' with fields for 'Phone Number' and 'Email Address'; and 'Reporting Party Relationship' with a dropdown menu. There are also fields for 'Reporting Party Signature' and 'Reporting Party Date'. The form is designed to be user-friendly and easy to fill out.

The data also includes details of how and when the illegal activity was carried out and any other information that may be useful. In doing so, it is very important to preserve all the evidence related to the complaint. After submitting the complaint, the applicant receives an e-mail message with confirmation of receipt, his name and password. Analysts review the complaint and forward the information to the competent state and/or international agencies and/or institutions for investigation.

IC3 does not conduct an investigation and therefore cannot provide the applicant with information about the investigative status of a previously filed complaint; complaint, once submitted to IC3, cannot be dismissed - annulled.

2.2 The European Cybercrime Center (EC3)

In January 2013, within EUROPOL, The European Cybercrime Center (EC3) was established with the aim of facilitating the enforcement of laws in the field of cybercrime within the European Union, which makes strategic decisions in the fight against cybercrime, informs the public about the work, supports and assists training, building new capacities, etc. EC3 has focused its efforts on helping citizens and member states through an online link as shown in Figure 2, sharing information with other Internet Complaint Centers in the world, and investing in the development of new technologies to improve the effectiveness of the fight against Internet crime.

As part of EUROPOL, the Internet Organized Crime Threat Assessment (IOCTA) was formed by EC3, with the aim of informing decision-makers in the fight against Internet crime at a strategic, tactical and political level. IOCTA provides information on the latest trends in Internet crime, highlights future risks and threats and makes recommendations to help the EU and its partners in their efforts to prevent the development of high-tech crime and reduce it to a socially acceptable minimum.

Figure 2. *Entry form of the complaint site (EC3)*



The areas that IOCTA pays the most attention and focuses on are:

- cyber attacks,
- sexual exploitation of children via the Internet,
- payment fraud.

3. Reports of international organizations

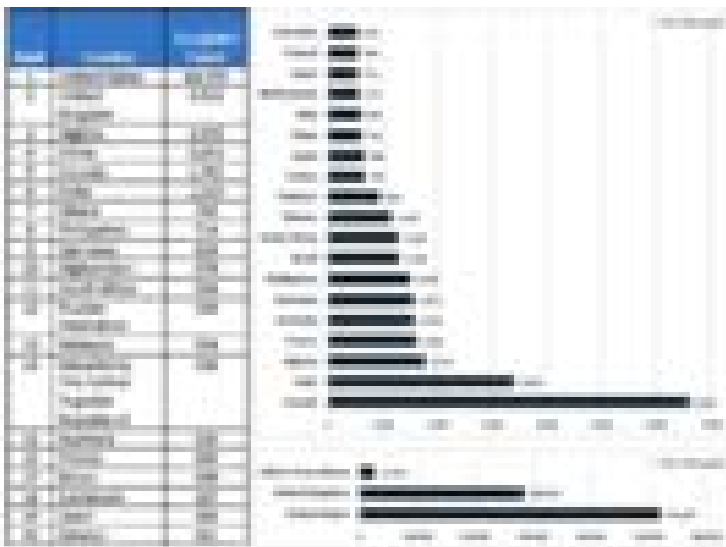
As we stated in the introduction of this paper, due to the limitation of the permitted scope of work, we will not deal with a detailed analysis of the data in the reports, the powerful tools of the two strongest and for us the most interesting centers IC3 and EC3. Using a comparative method of one type of the many types of reports presented there, we will only try to point out the usefulness of the work of the centers both in prevention and in synergistic work with other security agencies and law enforcement agencies, active and reactive support for victims, bearing in mind the indicated trend of using machine learning and artificial intelligence and their capabilities.

3.1 IC3 Report - Internet Crime Report

From the numerous annual reports of different types of IC3, as a representative example, for the goal we have set in this work, we will consider one that deals with the 20 countries with the largest number of reported incidents according to submitted complaints on the Internet, considering all countries from around the world, and showing them for 2013 - figure 3 and 2023 - figure 4.

Figure 3. 20 countries with the most complaints in the world in 2013.

Figure 4. 20 countries with the most complaints in the world in 2023.



3.2 Report EC3

Of the many reports of different types of EC3-IOCTA, we will give as a good example and deal with one that deals with the 10 biggest data compromises in the world by organizations, their work sector, the country they belong to and the number of compromised data. We will provide reports for 2015 - Figure 5 and for 2023 - Figure 6.

Figure 5. *Top 10 data breaches in the world in 2015.*

Figure 6. *Top 10 data breaches in the world in 2023.*

Organisation	Industry	Country	Records compromised	Organisation name	Sector	Location	Known records breached
Talk Talk	Telecoms	UK	4 000 000	DarkBeam	Cyber security	UK	>3,800,000,000
AdultFriendFinder	Other	Global	3 800 000	Real Estate Wealth Network	Construction/ real estate	USA	1,523,776,691
Moonpig Ltd	Technology	UK	3 600 000	Indian Council of Medical Research (ICMR)	Healthcare	India	815,000,000
Vivanuncios	Technology	UK	2 000 000	Kid Security	IT services/ software	Kazakhstan	>300,000,000
TV Channel MyTF1	Media	FR	1 900 000	Twitter (X)	IT services/ software	USA	>220,000,000
Scout Association	Other	UK	450 000	TuneFab	IT services/ software	Hong Kong	>151,000,000
MAPP.NL	Retail	NL	157 000	Dori Media Group	Media	Israel	>100 TB*
French State TV	Media	FR	108 000	Tigo	Telecoms	Hong Kong	>100,000,000
Army & Airforce Exchange (Siga Telecom)	Government	DE	98 000	SAP SE Bulgaria	IT services/ software	Bulgaria	95,592,696
World Trade Organization	Financial	Global	53 000	Luxottica Group	Manufacturing	Italy	70,000,000
CISI	Financial	UK	40 000				
Temporis	Other	FR	24 000				
British Airways	Transportation	UK	10 000				
PaymyPCN.net	Other	UK	10 000				

4. Discussion and concluding remarks

The rather small volume of data analyzed in this paper, from the considered only two of the several types of IC3 and EC3 reports shown in the previous subsections of the paper, and that by the simplest of the large number of powerful current tools of statistical and analysis by machine learning (Apruzzese et al., 2022) – by simple comparative analysis in different years, indicate the increasing and otherwise enormous popularity of the Internet. From the considered reports of IC3, through comparative analysis we easily come to the following conclusion about the worryingly high and growing number of reported crimes on the Internet, the number of which is higher in more developed countries, which is logical (UNSW, 2024; EUROPOL, 2015). Also, a comparative analysis of the second type of report from EC3 concludes that the number of compromised data is stagnant and that this is more pronounced in the most developed countries of the world, which, among other things, speaks of the organizationally and functionally good position of the institutions in the world that are at the forefront of the

fight against cybercrime, as well as of the expediency of the existence and operation of Internet complaint centers, with a primarily preventive role, and whose work in synergy with CERT and law enforcement authorities should be further encouraged.

REFERENCE LIST

- Aggestam, L. and Hyde-Price, A.G.V. *Security and Identity in Europe : Exploring the New Agenda*. New York USA: St. Martin's Press. 2000.
- Tuchman, J. Redefining Security. *Foreign Affairs* 1989. 68(2): 162-177.
- Varghese, M.; Raj, S.; Venkatesh, V. (2022). *Influence of AI in human lives*. Available at: www.researchgate.net/publication/366587833_Influence_of_AI_in_human_lives
- Randelović, M. et al. One aggregated approach in multidisciplinary based modeling to predict further students' education *Mathematics* 2022. 10 (14).
- Randelovic, D.; Randelovic, M.; Cabarkapa, M. Using Machine Learning in the Prediction of the Influence of Atmospheric Parameters on Health. *Mathematics* 2022. 10 (17).
- A. Aleksić, M. Randelović and D. Randelović. Using Machine Learning in Predicting the Impact of Meteorological Parameters on Traffic Incidents, *Mathematics* 2023. 11(2).
- Velasco, C. Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum23* 2022. <https://doi.org/10.1007/s12027-022-00702-z>.
- Ciancaglini, V. et al. *Malicious Uses and Abuses of Artificial Intelligence*. London United Kingdom: Trend Micro research. 2020.
- Brar, H.S.; Kumar, G. Cybercrimes: A Proposed Taxonomy and Challenges, *Journal of Computer Networks and Communications* 2018, Article ID 1798659, 11 pages, <https://doi.org/10.1155/2018/1798659>
- https://sr.wikipedia.org/sr-ec/Tipovi_kriminala_na_internetu Accessed on 20.04.2024.
- Sajid, A.. A Taxonomy of Cyber-attacks on Computer Networks. Bredford UK: University of Bradford. 2020. hal-02561057 <https://doi.org/10.1016/j.accinf.2020.100467>.
- <https://nordvpn.com/cybersecurity/glossary/attack-taxonomy/> Accessed on 20.04.2024.
- Rapid7. (2019). *Common Types of Cybersecurity Attacks and Hacking Techniques*. Available at: <https://www.rapid7.com/fundamentals/types-of-attacks/> Accessed 16.12.2023.
- Babic,I.;Miljkovic,A.;Cabarkapa,M.;Nikolic,V.;Đordjevic,A.;Randjelovic,M.;Randjelovic, D. Triple Modular Redundancy Optimization for Threshold Determination in Intrusion Detection Systems. *Symmetry* 2021. 13, 557. <https://doi.org/10.3390/sym13040557>
- Maksimović, A.; Nikolic, V.; Vidojević, D.; Randjelovic, M.; Djukanović, S.; Rand-

jelovic, D. Using Triple Modular Redundancy for Threshold Determination in DDOS Intrusion Detection Systems. *IEEE Access* 2022. PP. 1-1. 10.1109/ACCESS.2024.3384380.

<https://www.appsecengineer.com/blog/the-biggest-cyber-attacks-in-the-last-20-year> Accessed on 20.04.2024.

Stewart, E. *Top 10 Biggest Cyber Attacks in History*. Available at: <https://em360tech.com/top-10/top-10-most-notorious-cyber-attacks-history> Accessed on 20.04.2024.

Darijević, V. Sajber kriminal kao bezbednosni rizik na internetu. *Megatrend revija* 2021. Vol. 18, № 2, 257-266.

Službeni list SRJ – Međunarodni ugovori, br. 13/2002.

Službeni glasnik RS, br. 12/1996.

Nedeljković, S.; Randelović, D.; Kuk, K.; Nikolić, V. Internet centri za žalbe građana i sajber kriminal, VIII naučno-stručni skup „*Policija i pravosudni organi kao garanti slobode i bezbednosti u pravnoj državi*“, 23-25. maj 2017. Tara, Srbija.

Randelović, D.; Carević, B.: Uloga centara za žalbe na Internet kriminal u SAD u zaštiti ljudskih prava, *Kultura polisa*, specijaln broj sa KPA, 2012.

Apruzzese, G. et al. (2022). *The Role of Machine Learning in Cybersecurity*. 10.48550/arXiv.2206.09707.

<https://www.unsw.edu.au/newsroom/news/2024/04/World-first-Cybercrime-Index-ranks-countries-by-cybercrime-threat-level> Accessed on 20.04.2024.

<https://www.europol.europa.eu/iocta/2015/distribution.html> Accessed on 20.04.2024.

*Rejani Thudalikunnil Gopalan*¹

HUMAN TRAFFICKING: ENTRAPMENT METHODS AND FORENSIC INVESTIGATIONS

Abstract

Human trafficking is a growing problem in the world and it mainly violates human rights. The definitions of human trafficking principally focus on three components that are acts, means and purpose, and many types are identified, such as Labour Trafficking, Sex Trafficking, Child Trafficking, Bonded Labour, Forced Marriage and Organ Trafficking. Recently researchers have focused on various entrapment methods used by human traffickers, which span from physical and emotional abuses, threats, and isolation to seducing the victims. Depending on the type of trafficking, different entrapment methods or tactics are used by the traffickers. Forensic investigations related to human trafficking are also very challenging. This paper will explore various entrapment methods and forensic investigation methods as well as their challenges.

Keywords: *human trafficking, entrapment methods, forensic investigations, labour trafficking, sex trafficking, organ trafficking.*

HUMAN TRAFFICKING

Human trafficking is a growing problem and according to the UN Trafficking in Persons Protocol (2000), it is defined as "the recruitment, transport, transfer, harbouring or receipt of a person by such means as threat or use of force or other forms of coercion, abduction, fraud or deception for the purpose of exploitation". This exploitation can be in terms of sexual exploitation, forced labour, domestic servitude, child begging or the removal of organs. Human trafficking is different from human smuggling in terms of consent. More specifically, human smuggling happens with the consent of the individual but consent is absent in human trafficking and it is considered to be an act of human violation and modern slavery. The 2022 report of the International Labour Organisation (ILO), IOM and the Walk Free Foundation (WFF) estimated that 50 million people were victims of modern slavery on any given day in 2021 and that 27.6 million people were in situations of forced labour while another 22 million people were in a forced marriage.

Human trafficking is not the same as human smuggling. Human smuggling is consensual, whereas trafficking is done against a person's will (Rothman, 2017). There are three common types of human trafficking: the sex trade, forced labour, and domestic

¹ School of Special Education & Clinical Psychology, Apex University, Jaipur, India

servitude. The economic sectors that profit most from human trafficking are agriculture, restaurants, manufacturing, domestic work, entertainment, hospitality, and the commercial sex industry. Trafficking can occur between countries or in areas within a country (Eccleston, 2013). It can happen to anyone of any gender, race, or age (NHTH, 2017).

ENTRAPMENT METHODS

Many entrapment methods have been used for human trafficking and some of the most widely reported are based on relationship establishment with the targeted victim and on using aversive methods. The trafficker tries to manipulate the vulnerabilities, mainly the social and emotional risks of the victims. The entrapment methods can be headed under relational tactics (romantic partner, befriending) and aversive methods.

Relational tactics

1. Romantic partner

This method has been widely used to entrap the victim as reported by many studies. Many reviews and secondary data analyses consistently point out the fact that the traffickers target the victims and try to establish a romantic or boyfriend relationship with the victims and eventually traffic them. Reid (2016) reported in a review of 43 cases of sexually exploited girls that sex traffickers use numerous scripts and schemes such as boyfriend/lover scripts to entrap and entangle the victims. Twis, Gillespie, & Greenwood (2022) reported a similar finding. They analysed the secondary case files of 38 domestic minors who were trafficked for sex by their romantic partners in one state in the United States between 2012 and 2017. They concluded that environmental circumstances, such as gang involvement and family systems involvement often influenced victims trafficked by romantic partners. They use specific recruitment tactics to entrap and control their victims, like care giving, sexual or psychological violence. Moore et al (2020) observed an established relationship between domestic sexually trafficked victims and traffickers in a majority of the samples in their study. Baird & Connolly (2023) studied 23 original research with quantitative or qualitative data on the recruitment or pathways into sex trafficking for minors trafficked within the US and Canada from 1990 to 2020 and concluded that the Boyfriend scheme (i.e., "Romeo pimping") is most commonly cited tactic in which boyfriend recruiters/traffickers "sell the dream" of life together. They groom the victims with extra attention, care, love, gifts, money and in some cases drugs and once the victims are under their control they shift from romance to exploitation through manipulation and force.

2. Befriending

Many studies have reported that befriending is another method for entrapping victims of human trafficking, especially in the case of sexual purposes. "Befriending" tactic may include other girls working for trafficker pose as friend in recruitment, or friends may normalize selling sex, operate as a role model in sex trade, or use peer pressure to get youth to sell sex (Baird & Connolly, 2023). In many cases, it has been reported that traffickers use their victims for recruiting other victims either by manipulation or giving the task of recruiting others with proper training. The success of this method is also based on peer pressure and peer influence as the peers are posing as recruiters and normalising sex selling as a way to make quick money or to get drugs (Edinburgh et al., 2015; Cavazos, 2015; Reid, 2016; Moore et al., 2020).

3. Familial pimping

Family members, especially stepfather or mother (familial traffickers) force the child to get into sexual activity for earning and may lead to human trafficking. "Familial pimping" is the most coercive type of relationship, with parental authority and family loyalty acting as coercive strongholds over the child (Marcus et al., 2014) and, in some cases, traffickers act like parenting (Smith et al., 2009).

4. Aversive tactics

The core feature of these tactics is generating fear in the victims either through blackmail, financial abuse, pushing sexual boundaries, abduction, torture, drugging, gang rape, removing youths' identification, threats, and sexual violence in forcing youth to have sex with men for money (Baird & Connolly, 2023). In romantic strategy, aversive tactics were used in later stages in many cases but in Gorilla/Guerilla pimps or strategy aversive tactics were used from the beginning such as abduction, torture, drugging, gang rape, removing youths' identification, threats, and sexual violence in forcing youth to have sex with men for money, blackmailing and sexual assault for conditioning to nonconsensual sex (Baird et al., 2020; Dalley, 2010; Bruhns et al., 2018; Roe-Sepowitz, 2019).

Enmeshment factors

Several factors contribute to prolonged exploitation, which can be termed as enmeshment factors that can be control factors, dependency factors (these are trafficker-related factors) and youth factors for prolonging the exploitation or preventing it. Control tactics include fear, shame, feeling "owned", experiencing threats, intimation, blackmail, systemic isolation, trauma bond, and loyalty to the trafficker, rape, burnings,

violence, psychological abuse, intimidation, withholding documents, threats to the youth or their family's life, impregnating the youth, and threatening their pregnancy or child (Anderson et al., 2014; Nixon et al., 2002; Baird & Connolly, 2023), and systematic isolation by the trafficker (Bruhns et al., 2018; Cavazos, 2015). Another controlling factor is the trauma bond between the trafficker and victim in which the victim hopes for love and intimacy even after the violence recurs that may lead to the feeling of obligation and responsibility for the trafficker, which sometimes prevents the abuser from the criminal justice system (Smith et al., 2009; Reid, 2016; Rosenblatt, 2014).

The victims are unable to leave the situation due to dependency factors such as the trafficker nurturing drug addiction, and the trafficker is sole provider of basic needs, pregnancy, and debt bondage (Baird & Connolly, 2023; Dalley, 2010). The youth factor also resisting to leave the trapped situation which could be the relationship or attachment of the victim with the trafficker or the victim's need or longing for love and dependency (Baird & Connolly, 2023; Cecchet & Thoburn, 2014).

Social network and trafficking

Recently social networks have been used as a way to target the victims of human trafficking; social media like Facebook and Instagram are widely used for this purpose. The victims include women, men, and children, and they are usually trapped in situations like getting offers of fake jobs through social media (Gopalan, 2022). According to Europol (2016), human traffickers utilize technologies for recruiting, controlling, and transporting the victims and grooming of victims can happen through social media, especially if victims share their personal information and videos (Terwilliger, 2021; Reid, 2015; Moore et al., 2020). Social networks have been used for labour trafficking and the promise of high wages for a relatively simple job, free housing and transportation to the country in question as well as limited requirements of the candidates are the indicators for trafficking (Janusauskiene, 2013).

Psychosocial factors

Many psychosocial factors are associated with trafficking and many of the researches focused on the vulnerabilities of the victims. Those who come with a history of abuse and violence in childhood, community violence victimizations (Franchino-Olsen et al., 2022), high rates of alcohol or substance use/abuse, being placed in a group home or child protective services (CPS) custody, a history of runaway behaviour and/or exposure to other child maltreatment (Moore et al, 2020); gang membership, violence victimization, delinquency (Franchino-Olsen, H., & Martin, 2022) were found to be significantly associated with high risk for trafficking.

Forensic Investigations

Multimodal approach, which means the application of multiple Forensic Science techniques, is useful for the investigation of human trafficking. Forensic evaluations are important steps to assist the victim, including forensic medical and psychiatric evaluations. Forensic Science can aid to combat human trafficking in several ways such as finding and recognizing missing persons alive or dead, detection of victims of trafficking in persons, distinction of human trafficking from other crimes, identification of suspects, provision of proof in support of arrest, prosecution and conviction of perpetrators, thereby reducing the burden of victim testimony in court and authentication of travel documents (Sust, 2021).

Forensic Medical Evaluation

Forensic medical examinations help to establish the facts related to the allegation of trafficking to identify perpetrators and contribute to the procedures designed to obtain redress for the victims and it is performed at the request of bodies of investigation like court (Alempijevic, Jecmenica, Pavlekic, Savic & Aleksandric, 2007; Sust, 2021). It is important to conduct a detailed medical examination from head to toe by using laboratory and medical imaging techniques, textual and photographic documentation, and search for malnutrition, vitamin deficiency or other effects caused by inhuman treatment and slave-like living conditions; systematic collection of forensic samples (e.g. swabs, hair, blood, urine); forensic age diagnostics; dental status assessment; and screening for sexually transmitted diseases and other infections (Keatley & Clarke, 2019). Such detailed medical examination may assist or give clues for the type of trafficking. Studies have indicated that rashes and tattoos indicate sex trafficking while burns, injuries, and deep cuts were more likely to be found in labour-trafficked patients (Rambhatla et al., 2021).

Forensic Psychiatric Evaluation

Forensic psychiatric evaluation is important as many of the victims undergo trauma and emotional disturbances due to trafficking experiences. In addition to this, evaluation may give clues for the possibility of trafficking in terms of physical, behavioural and environmental aspects. Hence a trained psychiatrist or psychologist must perform forensic psychiatric evaluation. It is suggested by researchers that experts utilize the 6 principles of trauma-informed approach when evaluating any patient with suspected trafficking experience which emphasises safety, trustworthiness and transparency, peer support, collaboration and mutuality, empowerment, voice and choice, and cultural, historical and gender issues (Baldwin, Fehrenbacher & Eisenman, 2014; Alhajji & Hadjikyriakou, 2021). The tool used for evaluation is PEARR tool (2019), which emphasises privacy, educating the patient about abuse, ask or screen the patient for abuse, neglect or violence, and respect and respond the victim.

Forensic investigation methods/techniques

The forensic investigation in human trafficking utilizes all forensic science branches and methods as human trafficking is a combination of crimes. Apart from the major contributions from medical, psychology and psychiatry fields, digital technologies and digital forensics, forensic chemistry, forensic microbiology, biometrics, forensic archaeology, and forensic anthropology support heavily in the investigation related to human trafficking. UNODC (2009) mentioned about the types of physical evidences which can be used for forensic investigations such as blood, semen, skin cells, tissues, organs, muscle, bone, teeth, hair, saliva, fingernails, urine, etc. DNA analysis, finger and body marks (feet and ear), fibres and other micro traces, teeth examination, facial recognition, iris recognition, analysis of chemicals, biometrics including dactyloscopy/fingerprints, as well as palm prints are also aid in human trafficking investigations. Another important area is document evidence in which illegal reproduction of identity and travel documents are important evidence of trafficking in persons and the documents can be counterfeited (reproduced as original) or forged (altered originals by adding, removing or substituting relevant information) and can be used for recruitment and transportation of the victims (Sust, 2021).

Recently, many tools have been used for detecting and investigating human trafficking all over the world, like Human Trafficking app in Russia. Safe Trip app was launched to detect possibility of human trafficking among immigrants, which monitor departure to safe arrival or to an emergency along their way (Keatley, 2020). Free2work mobile application used for providing information on companies and their ratings as well as their approach to forced labour (Latonero, 2011). Advanced Digital Forensics (ADF) Solutions offers automated forensic tools for digital investigations and is also the founder of the Anti-Human Trafficking Intelligence Initiative. DNA based tools are also there such as The Programme for Kids Identification with DNA Systems (DNAPROKIDS) developed in 2002-2004, which focuses on the worldwide identification of missing children.

Forensic investigations & challenges

Many factors pose challenges to the investigations of human trafficking. One of the important challenges faced by legal authorities is reluctance of the victims in reporting the case and disclosing about their trafficker, which hampers further investigations and criminal procedures. As human trafficking involves multiple crimes, multiple people, operates from multiple geographical areas including locations and countries, and all those involved are connected with multiple agencies and operations and may not be known to each other directly, investigation of human trafficking requires lots of collaborative works from multiple agencies. The lack of coordination among different investigative agencies and organizations in the same country and international level risk increase complexity of the investigations. Privacy protection is another major area of concern related to vic-

tims. It is really important to coordinate with legislation, policy makers, laboratories and databases as well as investigation agencies. Public awareness and training for professionals involved in examinations and investigations are also well recommended. The issues related to human trafficking are increasing all over the world but its detection and investigations are lagging behind coupled with lack of general awareness in public.

REFERENCE LIST

- Alempijevic, D., Jecmenica, D., Pavlekic, S., Savic, S., & Aleksandric, B. (2007). Forensic medical examination of victims of trafficking in human beings. *Torture*, 17(2), 117-21.
- Alhajji, L., Hadjikyriakou, M., & Padilla, V. (2021). Psychiatrists' Response to Human Trafficking. *Psychiatric Times*, 38(12), 55-58.
- Anderson P. M., Coyle K. K., Johnson A., Denner J. (2014). An exploratory study of adolescent pimping relationships. *The Journal of Primary Prevention*, 35(2), 113–117.
- Baird, K., & Connolly, J. (2023). Recruitment and Entrapment Pathways of Minors into Sex Trafficking in Canada and the United States: A Systematic Review. *Trauma, violence & abuse*, 24(1), 189–202. <https://doi.org/10.1177/15248380211025241>
- Baird, K., McDonald, K. P., & Connolly, J. (2020). Sex trafficking of women and girls in a southern Ontario region: Police file review exploring victim characteristics, trafficking experiences, and the intersection with child welfare. *Canadian Journal of Behavioural Science /Revue canadienne des sciences du comportement*, 52(1), 8–17.
- Baldwin, S.B., Fehrenbacher, A.E., & Eisenman, D.P. (2015). Psychological Coercion in Human Trafficking: An Application of Biderman's Framework. *Qualitative Health Research*, 25(9):1171-1181. doi:10.1177/1049732314557087
- Bruhns, M. E., del Prado, A., Slezakova, J., Lapinski, A. J., Li, T., & Pizer, B. (2018). Survivors' perspectives on recovery from commercial sexual exploitation beginning in childhood. *The Counseling Psychologist*, 46(4), 413–455. <https://doi.org/10.1177/0011000018777544>
- Cavazos, J. (2015). *The voices of domestic minors trafficked for commercial sexual exploitation within the United States: A qualitative retrospective study with a narrative approach*. Alliant International University.
- Cecchet, S., & Thoburn, J. (2014). The Psychological Experience of Child and Adolescent Sex Trafficking in the United States: Trauma and Resilience in Survivors. *Psychological Trauma: Theory, Research, Practice, and Policy*. 6. 482-493. 10.1037/a0035763
- Dalley, M. (2010). *The domestic trafficking of children in Canada: The relationship to sexual exploitation, running away and children at risk of harm*. <https://www.public-safety.gc.ca/lbrr/archives/cnmcs-plcng/cn30898-eng.pdf>

- Eccleston D. (2013). Identifying victims of human trafficking. *Community practitioner: the journal of the Community Practitioners' & Health Visitors' Association*, 86(5), 40–42.
- Edinburgh, L., Pape-Blabolil, J., Harpin, S. B., & Saewyc, E. (2015). Assessing exploitation experiences of girls and boys seen at a child advocacy center. *Child Abuse & Neglect*, 46, 47–59.
- Europol. (2016). Situation Report: *Trafficking in Human Beings in the EU*. The Hague: Europol. Available at: <https://www.europol.europa.eu/publicationsdocuments/>
- Franchino-Olsen, H., & Martin, S. L. (2022). The Associations between Gang Membership and Domestic Minor Sex Trafficking: Findings From a Nationally Representative Study. *Violence and victims*, 37(4), 479–496. <https://doi.org/10.1891/VV-2021-0070>
- Franchino-Olsen, H., Martin, S. L., Halpern, C. T., Preisser, J. S., Zimmer, C., & Shanahan, M. (2022). Adolescent Experiences of Violence Victimization Among Minors Who Exchange Sex/Experience Minor Sex Trafficking. *Journal of interpersonal violence*, 37(17-18), NP16277–NP16301. <https://doi.org/10.1177/08862605211021967>
- Gopalan, R.T. (2022). Social networks and human trafficking. In Boskovic, M., Misev, G., & Putnik, N. (Ed.), *Analyzing New Forms of Social Disorders in Modern Virtual Environments* (1st ed., pp. 66-98). IGI Global. DOI: 10.4018/978-1-6684-5760-3.ch004.
- How to Navigate a Human Trafficking Investigation* (2022). <https://www.sound-thinking.com/blog/how-to-navigate-a-human-trafficking-investigation/>
- Janusauskiene, D. (2013). Lithuanian Migrants as Victims of Human Trafficking for Forced Labour and Labour Exploitation Abroad. In *Exploitation of Migrant Workers in Finland, Sweden, Estonia and Lithuania: Uncovering the Links between Recruitment, Irregular Employment Practices and Labour Trafficking*. Helsinki: European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI).
- Keatley, D. (2020). *The Timeline Toolkit Australia*: ReBSA Publications.
- Latonero M. (2011). *Human trafficking online: The role of social networking sites and online classifieds*. Available at SSRN 2045851
- Marcus, A., Horning, A., Curtis, R., Sanson, J., & Thompson, E. (2014). Conflict and agency among sex workers and pimps: A closer look at domestic minor sex trafficking. *The ANNALS of the American Academy of Political and Social Science*, 653(1), 225–246.
- Moore, J. L., Houck, C., Hirway, P., Barron, C. E., & Goldberg, A. P. (2020). Trafficking Experiences and Psychosocial Features of Domestic Minor Sex Trafficking Victims. *Journal of interpersonal violence*, 35(15-16), 3148–3163. <https://doi.org/10.1177/0886260517703373>
- NHTH. (2017). *Hotline*. Retrieved July 2017 from [https:// humantraffickinghotline.org/audience/service-providers](https://humantraffickinghotline.org/audience/service-providers)
- Nixon K., Tutty L., Downe P., Gorkoff K., Ursel J. (2002). The everyday occurrence: Violence in the lives of girls exploited through prostitution. *Violence against Women*, 8(9), 1016–1043.

Rambhatla, R., Jamgochian, M., Ricco, C., Shah, R., Ghani, H., Silence, C., Rao, B., & Kourosh, A. S. (2021). Identification of skin signs in human-trafficking survivors. *International journal of women's dermatology*, 7(5Part B), 677–682. <https://doi.org/10.1016/j.ijwd.2021.09.011>

Reid, J. A. (2015). *Sex trafficking of girls: How sex traffickers exploit youth and system vulnerabilities*. In Paper presented at the anti-trafficking initiative lecture series. Washington University in St. Louis. Retrieved from [https:// digital.usfsp.edu/fac_publications/217/](https://digital.usfsp.edu/fac_publications/217/)

Reid J. A. (2016). Entrapment and Enmeshment Schemes Used by Sex Traffickers. *Sexual abuse: a journal of research and treatment*, 28(6), 491–511. <https://doi.org/10.1177/1079063214544334>

Roe-Sepowitz, D. (2019). A six-year analysis of sex traffickers of minors: Exploring characteristics and sex trafficking patterns. *Journal of Human Behavior in the Social Environment*, 29(5), 608–629.

Rosenblatt, K.(2014). Determining the vulnerability factors, lures and recruitment methods used to entrap American children into sex trafficking. *Sociology and Criminology-Open Access*, 1-15.

Rothman, E. F., Stoklosa, H., Baldwin, S. B., Chisolm-Straker, M., Kato Price, R., Atkinson, H. G., & HEAL Trafficking (2017). Public Health Research Priorities to Address US Human Trafficking. *American journal of public health*, 107(7), 1045–1047. <https://doi.org/10.2105/AJPH.2017.303858>

Smith, L. A., Healy Vardaman, S., & Snow, M. (2009). *The national report on domestic minor sex trafficking: America's prostituted children*. Shared Hope International.

Sust, L. (2021). *Forensic science in combat of human trafficking*. Murdoch University. Master thesis, 1-122.

Terwilliger, A. M. (2021). *The Role of social media in Human Trafficking Victimization* [Doctoral dissertation]. Nova Southeastern University. [https:// nsuworks.nova.edu/fse_etd/323](https://nsuworks.nova.edu/fse_etd/323)

trafficking-in-human-beings-in-eu

Twis, M. K., Gillespie, L., & Greenwood, D. (2022). An Analysis of Romantic Partnership Dynamics in Domestic Minor Sex Trafficking Case Files. *Journal of interpersonal violence*, 37(7-8), NP5394–NP5418. <https://doi.org/10.1177/0886260520960302>

UN General Assembly. (2000). Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the United Nations Convention against Transnational Organized Crime. Available at: <https://www.ref-world.org/docid/4720706c0.html>

UNODC. Crime scene and physical evidence examinations in trafficking in persons investigations. Anti-human trafficking manual for criminal justice practitioners Module 7. 2009.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

911.3::327]:355.02(100)"20"(082)(0.034.4)
327(100)"20"(082)(0.034.4)

INTERNATIONAL Scientific Conference - BINS 2024 Challenges of military neutrality
in dynamic geopolitical relations (2024 ; Belgrade)

Conference proceedings [Електронски извор] / International Scientific Conference
- BINS 2024 Challenges of military neutrality in dynamic geopolitical relations,
Belgrade, May 22, 2024 ; [editor Milica Bošković]. - Belgrade : Faculty of Diplo-
macy and Security, 2025 (Belgrade : Faculty of Diplomacy and Security). - 1 USB
fleš memorija : tekst ; 1 x 3 x 8 cm

Sistemski zahtevi: Nisu navedeni. - Tiraž 100. - Str. 7: Uvodnik / Milica Bošković

ISBN 978-86-87545-50-2

- а) Геополитика -- Војни аспект -- 21в -- Апстракти
- б) Геополитика -- Војни аспект -- 21в -- Зборници
- в) Међународни односи -- 21в -- Зборници

COBISS.SR-ID 165807369



Republic of Serbia
MINISTRY OF
FOREIGN AFFAIRS



FDB

FACULTY OF
DIPLOMACY
AND SECURITY



BINS 2024

SECURITY CHALLENGES OF
THE NEW WORLD



SDASU TV
www.SDASU.tv

Štamperija
beopres