FDB FACULTY OF DIPLOMACY AND SECURITY

INTERNATIONAL SCIENTIFIC CONFERENCE

BINS 2025
SECURITY CHALLENGES OF THE NEW WORLD

Co-funded by the European Union

TRANSDISCIPLINARITY OF SECURITY STUDIES AND PRACTICES

CONFERENCE PROCEEDINGS

Belgrade, May 8 - 9, 2025

INTERNATIONAL SCIENTIFIC CONFERENCE

BINS 2025

TRANSDISCIPLINARITY OF SECURITY STUDIES AND PRACTICE

FACULTY OF DIPLOMACY AND SECURITY
Belgrade, 2025.

INTERNATIONAL SCIENTIFIC CONFERENCE - BINS 2025

CONFERENCE PROOCEEDINGS

TRANSDISCIPLINARITY OF SECURITY STUDIES AND PRACTICE

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:
Mina Suknović, MA

Translation:
Doc. Dr. Katarina Šmakić

E-edition:
Faculty of Diplomacy and Security, Belgrade

Circulation:
100 copies

ISBN-978-86-87545-51-9

Belgrade, 2025.

INTERNATIONAL SCIENTIFIC CONFERENCE - BINS 2025

TRANSDISCIPLINARITY OF SECURITY STUDIES AND PRACTICE

FACULTY OF DIPLOMACY AND SECURITY
BELGRADE, MAY 8-9, 2025.

CONTENT

FOREWORD

Inspired by the project under which this conference is being held, the fact that we have gathered to provide answers to current and emerging threats, and taking into account the accreditation of the joint master's program *Gender and Security*, I would now like to briefly highlight the importance of education for security, equality, and the development of societies and states.

In academic literature, both contemporary and from the 20th century, it is emphasized that, among other things, two primary goals of education are to provide individuals with knowledge and skills that are essential for their engagement in social and political life and for their economic advancement. Today, an increasingly important goal is also to equip people for successful social mobility. It is indisputable that education should enable individuals to develop critical thinking and achieve their desired socio-economic goals and status. The right to education is one of the fundamental human rights. However, even though this right is enshrined in the highest documents of international organizations and national legislations, this does not necessarily mean that it is fully realized in practice.

Diversity of knowledge and a high level of education are among the key factors in determining individuals' socio-economic status, raising awareness of human rights, and - when combined with access to healthcare and a healthy environment - contribute to a greater sense of security among individuals and communities, and thus to the overall security of the state.

Without education, healthcare, and justice that are equally accessible to all, there can be no qualitative progress of society. Quantity without quality, in this context, means a kind of artificial inflation of economic and security indicators, while the benefits of such results are not equally felt by all. In such societies, violence and violent individuals often find justification for their aggression in stereotypes, and sometimes even support in parts of the society.

If we do not wish to rely solely on legislation and repression (which do not address the root causes), only quality education, the acquisition of life skills, and the development of awareness about the inviolability and unquestionable importance of equality can serve as the foundation and root of sustainable social development and a sense of safety for all.

In addition to scientific efforts, practical experience shows that there can be no social development, prosperity for citizens, or ultimately, security for all, without equality and inclusion. However, these require a highly developed social awareness of tolerance, diversity, and human rights - an awareness that cannot exist without high-quality and universally accessible education.

Prof. Dr. Milica Bošković

Veselin Mićanović[1]
Dijana Vučković[2]

ARTIFICIAL INTELLIGENCE AND ITS SECURITY IMPLICATIONS

Abstract

Artificial intelligence is a rapidly developing technology that has the potential to transform many sectors, including education, information transfer, finance, and the like. As artificial intelligence is increasingly integrated into everyday life, there is growing concern about its security implications. These implications can take many forms, from physical and cyber security to ethical challenges. The paper presents the security implications in the field of application of artificial intelligence, which provides: cyber security and system autonomy, privacy and surveillance, protection from addiction to the use of artificial intelligence and its abuse, increased responsibility. The aim of the paper is to highlight the importance of artificial intelligence and its security implications in various fields based on technology that enables computers and systems to perform tasks that usually require human intelligence, such as speech recognition, learning, problem solving and decision making. The security implications of artificial intelligence are serious and multifactorial, ranging from cyber threats to ethical dilemmas. In order to minimize potential risks, it is necessary to develop international standards and regulations that enable the safe use of artificial intelligence while ensuring transparency, accountability and protection of human rights. Also, education and awareness of risks on the part of users and decision-makers plays a key role in reducing potential negative consequences.

Keywords: *Artificial Intelligence, Cyber Security, Implication, System, Technology, Risk, Consequence.*

INTRODUCTION

Artificial intelligence has recently become a key technology that shapes society in all development domains. Although it has the potential to bring significant benefits, its security implications also pose a serious challenge that needs to be carefully considered (Cucu et al., 2019). Understanding the security aspects of artificial intelligence is essential for minimizing risk and maximizing benefits. Numerous research studies are dedicated to cyber security due to misuse of artificial intelligence as well as for enhancing protection

[1] Faculty of Philosophy, University of Montenegro, Podgorica, Montenegro, veselinm@ucg.ac.me

[2] Faculty of Philosophy, University of Montenegro, Podgorica, Montenegro, dijanav@ucg.ac.me

and identifying malware (Al-Khshali & Ilyas, 2023; Ullah et al., 2022). We will try to present some of the security implications of artificial intelligence through cyber security, privacy and surveillance, misinformation and manipulation, ethics, and excessive automation, but we will also explore measures to improve the artificial intelligence security.

SOME SECURITY IMPLICATIONS OF ARTIFICIAL INTELLIGENCE

The security implications of artificial intelligence are broad and include numerous aspects of society as a whole, its development and technology. The introduction of artificial intelligence into everyday systems brings many benefits, but also creates serious security risks and threats. Bahcecik analyzes various studies on the significance of AI's impact on global security and notes that they differ significantly in their historical horizons, analytical frameworks, and the dimensions they identify (Bahcecik, 2023). Understanding these implications is crucial for developing strategies to minimize hazards. As highlighted, the introduction of artificial intelligence into everyday systems brings significant advantages, such as efficiency, automation and improvement of the quality of services. The introduction of artificial intelligence into everyday systems brings numerous advantages that can significantly improve various aspects of life and work. Some of the key benefits include:

- Efficiency and productivity. Artificial intelligence can automate routine and repetitive tasks, freeing up time for people to focus on more creative and strategic activities. In industries such as manufacturing, logistics and administration, artificial intelligence can reduce human error and increase data processing speed, thereby improving overall efficiency. Federspiel et al. have an optimistic view of a future in which human workers will be largely replaced by AI, which will improve automation and productivity (Federspiel et al., 2023).
- Service personalization. Artificial intelligence enables the personalization of the user experience. For example, in customer support services, artificial intelligence can analyze user preferences and behavior to offer personalized recommendations thus improving the user experience.
- Improving the quality of service. Artificial intelligence can enhance the quality of services in various sectors. For example, in education, artificial intelligence can provide personalized educational tools that adapt to the needs of each student.
- Proactive problem-solving approach. Artificial intelligence can analyze large amounts of data in real time and detect patterns that may indicate potential problems. For example, in the maintenance industry, AI can predict when equipment or infrastructure will require repairs, thereby reducing downtime and maintenance costs.

- Security improvement. In many areas, artificial intelligence can help monitor security threats and provide early warnings. For example, in finance, artificial intelligence can detect suspicious transactions or fraud attempts, while in transportation, autonomous vehicles can reduce the number of traffic accidents.
- Development of new products and services. Artificial intelligence can accelerate innovation by analyzing market trends and user data, helping businesses develop new products or services that are better tailored to market needs.

The combination of these benefits can lead to significant improvements in business, public services, healthcare, education, and other areas. However, it is important that these systems are implemented with appropriate oversight and ethical guidelines to ensure security and fairness. Nevertheless, alongside its benefits, there are also serious security risks accompanying its development and application, such as:

- Artificial intelligence can be the target of hacker attacks. Attackers can exploit vulnerabilities in artificial intelligence algorithms or manipulate them to gain access to sensitive data or cause damage to systems.
- Artificial intelligence enables the creation of highly convincing false representations, which can lead to manipulation of information, dissemination of misinformation, or even deceptive practices for the purpose of fraud.
- In some situations, artificial intelligence can make decisions that are potentially harmful or unfair, especially if it is not transparently understandable or if there are biases in the data it was trained on.
- Artificial intelligence can be used to collect and analyze data about users, which jeopardizes the privacy of individuals and can be used for unacceptable surveillance or manipulation.
- In robotics, artificial intelligence can enable robots (machines) to make their own decisions. Inadequate supervision can lead to accidents or even sabotage.

In order to minimize the above risks, strategies are needed that include:

- Security measures: Developing strong security protocols to protect against attacks and ensure the integrity of artificial intelligence with the highest levels of protection.
- Transparency and accountability: Introducing clear guidelines for the development of artificial intelligence systems so that it is clear how and why decisions are made.
- Ethics in design: Incorporating ethical guidelines and principles into the development of artificial intelligence technologies to avoid bias and unfair consequences.
- Control and supervision: Ensuring that AI systems are under constant human supervision and can be corrected or shut down if an error occurs.
- Training and education: Raising awareness among users and developers about security challenges and ways to protect against them. Ultimately, balancing benefits and risks is key to the safe and responsible integration of artificial intelligence into our daily lives.

ARTIFICIAL INTELLIGENCE AND ITS IMPACT ON GLOBAL SECURITY

Artificial intelligence is having a profound and pervasive impact on global security, bringing both benefits and challenges. The development and application of technologies based on artificial intelligence across various sectors can significantly shape the dynamics of security in the world on every level. Perspectives and Protection Strategies address the ways in which artificial intelligence technology is shaping global security, both in the context of challenges and threats, and in terms of protection strategies that could mitigate potential risks. Considering the accelerated development of artificial intelligence, this impact is becoming increasingly significant and requires attention from all aspects - from cyber security to infrastructure protection and the preservation of mutual relations.

Artificial intelligence can analyze vast amounts of data and detect patterns that could indicate possible threats in different areas. Das and Sandhane researched the latest AI trends in cybersecurity in research papers over the past four years across different search engines (Das & Sandhane, 2021). Algorithms for risk recognition, analysis and data processing can help identify and prevent unwanted activities. In emergency situations, artificial intelligence can help predict events, analyze hazards and optimize responses, thereby preventing many undesirable effects. Artificial intelligence is used to protect critical infrastructure systems and its security monitoring algorithms can detect attacks or systems errors in time, and enable preventive measures.

One of the biggest challenges that artificial intelligence poses to global security is the use of autonomous systems for various attacks. Robots, drones and other autonomous technologies can take over decision-making in potential conflicts, increasing the risk of conflict escalation or poor decision-making in critical situations.

Considering that artificial intelligence and technologies play a key role in modern information systems, there is also a risk of artificial intelligence being used for sophisticated cyberattacks. Attacks on national security systems, economies and infrastructure can be faster, more precise and more effective than ever before. Artificial intelligence is used to generate fake news, fake footage and manipulate information. This can have a negative impact on information stability, increase social tensions and undermine trust in public institutions. Countries that are technologically advanced and possess powerful artificial intelligence and infrastructure can have a strategic advantage in international relations. This can lead to the creation of a global power imbalance, where countries that are unable to develop and use artificial intelligence and related technology remain vulnerable.

In order to reduce the negative impacts of artificial intelligence on security, it is important to develop international regulations and ethical guidelines for the development and application of these technologies. The EU pays serious attention to security perspectives in order to achieve as much digital sovereignty as possible in order to neutralize the existing traditional weaknesses (Calderaro & Blumfelde, 2022:424). Governments, international organizations and private companies must work together to create global frameworks for the use of artificial intelligence in security applications, such as cyber security.

Also, it is necessary to ensure accountability and transparency in the use of artificial intelligence in security operations. Ultimately, artificial intelligence has the potential to significantly contribute to global security, but its impact depends on how it is implemented and regulated in the future.

Artificial intelligence enables advanced data analysis and monitoring of large amounts of information in real time. Its use in mass surveillance can lead to violations of human rights, while misuse of this technology could destabilize society. Artificial intelligence is playing an increasingly significant role in cyber attacks. Attackers can use sophisticated algorithms for hacking, data theft, and system manipulation. This poses a significant threat to national security and global stability.

CHALLENGES IN PROTECTING PRIVACY IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE

The challenges in privacy protection in the context of artificial intelligence represent a serious problem in an era when artificial intelligence is becoming increasingly present in everyday life. Although artificial intelligence brings many benefits, such as improved efficiency and accuracy in various sectors, it also creates new threats and challenges in terms of protecting the privacy of individuals. Using artificial intelligence to analyze, store and process large amounts of data can jeopardize personal privacy and even lead to data misuse. The complexities posed by AI to data privacy, ethical considerations, and the dynamic nature of cyber threats necessitate adaptive strategies and interdisciplinary research efforts (Ghimire, 2024).

Privacy threats in the context of artificial intelligence can be observed through:

- Mass data collection where artificial intelligence often relies on vast amounts of data for training algorithms. This data can include information about users, their behavior, habits, locations, and even biometric data. Often this data are collected without sufficient safeguards or user consent, which can compromise privacy.
- Insufficient control over personal data, which can occur in a situation when user data become digitized and stored in various systems, and it is often difficult for users to have full control over that data. Artificial intelligence algorithms can analyze this data in ways that users cannot predict or understand, meaning they do not have full control over what happens to their personal information.

- Personal privacy in the context of surveillance where systems based on artificial intelligence enable constant monitoring of citizens. While this can be useful for improving security, it raises major privacy concerns as it allows mass surveillance of people's behavior and movements without their consent.
- Profiling and discrimination where artificial intelligence can use data to create precise user profiles. By using user data, artificial intelligence can make automated decisions about important aspects of life, without transparency or human control. In some cases, artificial intelligence can make discriminatory decisions based on unconscious biases, which can negatively affect an individual's privacy and rights.

Challenges in privacy protection in the context of artificial intelligence can be viewed through:

- Regulation and compliance with laws in such a way that one of the biggest challenges in privacy protection in the era of artificial intelligence is observed through the lack of universal laws and regulations. Although there are laws such as the General Data Protection Regulation in the European Union, which prescribe how user data should be handled, many countries do not have sufficiently strict laws. In addition, the global nature of the Internet makes it difficult to align laws across different jurisdictions.
- The lack of transparency in algorithms leads to data monitoring and control becoming difficult, which creates difficulties in ensuring privacy. Users are often unaware of what information is collected, how it is used, and who has access to it.
- Inefficient data management refers to the fact that the use of artificial intelligence can often be awkward or ineffective due to the use of large amounts of data associated with individuals. Even with appropriate protective measures in place, poor data management can lead to security breaches and exposure of personal information.
- Technical issues of data protection in terms of privacy protection, as it is very challenging to develop technologies that safeguard data at all stages - from collection to processing and storage. Also, advancements in cryptography and data protection technologies (such as encryption) often do not keep pace with advances in artificial intelligence, meaning that data can be vulnerable to cyber attacks.
- Improper use of data for commercial purposes is seen through the fact that many companies use artificial intelligence to analyze consumer data, and these data are often used to create personalized marketing campaigns. However, this may violate user privacy as sensitive information about their habits and behavior is used without sufficient consent or control.

Possible solutions and strategies for privacy protection in the context of artificial intelligence can be viewed through:

- Focusing on the "right to privacy" as a fundamental human right. It is necessary to direct global attention to the preservation of privacy as a fundamental human right. Lawmakers should continue to develop regulations that enable privacy protection, with appropriate controls and sanctions for violations.
- Developing "explainable" AI systems, which involves the development of artificial intelligence systems that are not only efficient, but also transparent. This means that AI should be designed so that it can explain its decisions in a manner that users can understand. This approach can help protect privacy and allow users to have more control over their data.
- The use of data protection technologies (encryption) can help reduce the risk of privacy breaches. Technologies such as homomorphic encryption or differential privacy allow data analysis without revealing personal information, thereby reducing the risk to users.
- Consent and data control by users. To protect privacy, users should be given better control over their data. This includes a clear and transparent policy on how their data are collected, used, and stored, with the possibility for users to withdraw consent or request deletion of their data at any time.
- Proper data management and data minimization. It is important to apply the principles of data minimization, which means that only the data necessary for the functionality of the system is collected. Also, it is important that data are regularly deleted when no longer needed.

Protecting privacy in the context of artificial intelligence is a complex challenge that requires a balance between the benefits that artificial intelligence can provide and the risks it poses to individual privacy. The issues arising from growing privacy concerns are the result of the negative implication of artificial intelligence on our digital privacy (Ghimire, 2024). Developing appropriate laws, transparent systems and data protection technologies, as well as ensuring control over personal information, is key to preserving privacy in the era of artificial intelligence.

PROTECTION STRATEGIES AND SOLUTIONS TO MINIMIZE THREATS

Artificial intelligence has enormous potential to shape the future of global security – either through benefits, such as improving efficiency in many sectors, or through new threats and risks. With responsible development, international cooperation, and strong regulation, it is possible to minimize risks and use artificial intelligence to improve global security “Although AI implementation in organisational cyber security is recognised for its ability to achieve efficiencies beyond human capabilities, there are several drawbacks associated with its adoption, particularly at the organisational level" (Jada & Mayayise, 2024:7). It is crucial to direct efforts towards ensuring security and protecting human rights in an era increasingly shaped by this technology.

In order to ensure international security, it is necessary to establish global standards and regulations that will govern the development and application of artificial intelligence. International organizations, governments, and defense systems should focus their efforts on reaching an agreement on controls on the development of autonomous systems and the use of artificial intelligence for security purposes. Also, it is important to coordinate data protection and privacy regulations.

The use of artificial intelligence must be based on ethics and responsibility. Ethical principles in the development of artificial intelligence should ensure that the technology is used in accordance with human rights and safely for society.There must be ethical obligations that companies must adhere to when implementing generative artificial intelligence, as there are potential cybersecurity risks that companies are exposed to because artificial intelligence is not accompanied by adequate security measures (Humphreys et al., 2024).

Directing resources towards protection against artificial intelligence-based cyber attacks is a key strategy. Developing sophisticated real-time attack detection and prevention systems using artificial intelligence can help stop cyber threats before they escalate into serious incidents. Also, investments in cybersecurity training for experts and development of automated tools for monitoring and protection against attacks are needed.

When artificial intelligence is used in critical sectors, such as manufacturing, healthcare, energy networks or transportation, it is important to implement appropriate security protocols and regularly test these systems. The goal is to ensure security, predict and prevent potential security risks through the use of artificial intelligence. Also, it is important to monitor the security of infrastructure systems used by artificial intelligence.

Developing tools and techniques for detecting harmful content, as well as recognizing false information generated by artificial intelligence, can help protect against numerous manipulations and disinformation. Increased efforts in preventing cyber manipulation and identifying fake news can significantly improve global security.

Protection against the threats of misuse of artificial intelligence implies education and training of experts and the general public. Education on security in the digital age, the ethics of artificial intelligence, and potential threats can help create resilient communities that are able to recognize and address the security challenges that arise with technological advancements.

SOLUTIONS TO REDUCE SECURITY THREATS

Security in the era of artificial intelligence requires a proactive approach that involves multidisciplinary efforts. In their work, Osoba and Welser (2017) deal with national and domestic risks in the field of security created by artificial intelligence. Threats are numerous and often evolve faster than appropriate security protocols can be adapted. However, with careful planning, global collaboration and responsible innovation, we can create an environment where the benefits of artificial intelligence will be maximized, while the risks will be minimized.

Developing and harmonizing international and national laws related to the development, implementation, and use of artificial intelligence is necessary for its further implementation. Clear ethical guidelines and legal frameworks should be established to ensure the responsible use of the technology.

One way to increase the security of artificial intelligence is through transparency and accountability in its development. This implies the development of a system whose decisions can be understood and verified by humans. It seems important to ensure greater responsibility for decisions made by artificial intelligence.

The development of artificial intelligence and protection systems against misuse for cyber threats (Dawson, 2021), e.g. the use of artificial intelligence in security protocols can help detect and prevent attacks more quickly. The use of security solutions based on artificial intelligence can improve the system's ability to recognize anomalies or attacks in real time.

In order to reduce security threats, it is necessary to organize additional education and training of users, it is necessary to educate and train experts in the field of security and artificial intelligence. Only with proper knowledge and education, experts can identify potential threats in a timely manner and implement appropriate protection measures.

These priorities are also recognized in the recommendations outlined by the European Council, which deal with the improvement of technological capacities and the preservation of European values to achieve greater security (European Council 2020). Introducing ethical guidelines into the process of designing and implementing artificial intelligence can contribute to reducing the negative consequences of technology. Responsible development must include concern for potential harm, safety and well-being of users.

CONCLUSION

Artificial intelligence holds enormous potential to improve various sectors of society, from healthcare and education to security and the economy. However, with these advances come significant security challenges. Growing application of artificial intelligence in critical systems, such as education, food production, economy, military industry, etc. creates new vulnerabilities that can be exploited.

Artificial intelligence holds tremendous potential to enhance various sectors of society, from healthcare and education to security and the economy. However, with this progress come significant challenges concerning security. The growing application of artificial intelligence in critical systems, such as education, food production, the economy, the military industry, and others, creates new vulnerabilities that can be exploited.

One of the biggest risks lies in the possibility of artificial intelligence becoming a tool for cyber attacks or to be used for malicious purposes, such as the creation of false information (deepfake), automated system hacking or market manipulation. Also, artificial intelligence can lead to a reduction in the human role in decision-making, which can raise ethical and legal dilemmas, including liability for mistakes made by an algorithm.

Given these challenges, it is important to develop international regulations and standards that will enable the responsible and safe use of artificial intelligence. Along with technological advancements, it is crucial to invest in training and education to reduce the possibility of misuse. In addition, the impact of artificial intelligence on security must be continuously monitored and evaluated, and protection and liability strategies must be adjusted accordingly.

Ultimately, in order for artificial intelligence to be safer and more useful, it is necessary to establish a balance between innovation and security measures, while continually improving technological supervision and ethical standards in its application.

REFERENCE LIST

Al-Khshali, H. H., & Ilyas, M. (2023). Impact of portable executable Header features on malware detection accuracy. *Computers, Materials & Continua*, 74(1), 153–178. https://doi.org/10.32604/cmc.2023.032182

Bahcecik, S. O. (2023). I TRENDS Security Politics and Artificial Intelligence: Key Trends and Debates. *International Political Science Abstracts*, 73(3), 329-338.

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security*, 31(3), 415-434.

Cucu, C., Gavrioloaia, G., Bologa, R., & Cazacu, M. (2019). *Current technologies and trends in cybersecurity and the impact of artificial intelligence* (Vol. 2). eLearning & Software for Education.

Das, R., & Sandhane, R. (2021). Artificial intelligence in cyber security. In *Journal of Physics: Conference Series* (Vol. 1964, No. 4, p. 042072). IOP Publishing.

Dawson, M. (2021). Cybersecurity impacts for artificial intelligence use within industry 4.0. *Scientific Bulletin*, 26(1), 24–31.

European Council (2020). *European Council conclusions*, 1-2 October 2020.

Federspiel, F., Mitchell, R., Asokan, A., Umana, C., & McCoy, D. (2023). Threats by artificial intelligence to human health and human existence. *BMJ Global Health*. 2023;8:e010435. doi:10.1136/bmjgh-2022-010435

Ghimire, S. (2024). *Artificial intelligence and its implications to digital security*. Frost & Sullivan Institute. https://frostandsullivaninstitute.org/wp-content/uploads/2024/02/Artificial-Intelligence-and-Its-Implications-to-Digital-Security.pdf

Humphreys, D., Koay, A., Desmond, D., & Mealy, E. (2024). AI hype as a cyber security risk: The moral responsibility of implementing generative AI in business. *AI and Ethic*s, 4(3), 791-804.

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, 8(2), 100063.

Osoba, O. A., & Welser, W. (2017). *The risks of artificial intelligence to security and the future of work*. Santa Monica, CA: RAND.

Ullah, F., Alsirhani, A., Alshahrani, M. M., Alomari, A., Naeem, H., & Shah, S. A. (2022). Explainable malware detection system using transformers-based transfer learning and multi-model visual representation. *Sensors*, 22(18). https://doi.org/10.3390/s22186766

Hossam Nabil Al Shenraky[1]

EDUCATION AND CAPACITY BUILDING IN CYBERCRIME INVESTIGATION STUDIES

Abstract

Given the pace of development in cyber threats, training in cybercrime investigation needs to be transformative and complemented by cutting-edge capacity-building strategies. The present study attempts to explain how transdisciplinary frameworks further train and equip professionals to handle contemporary cybercrime-related issues. It brings together topics such as information technology, law, behavioral science, and cybersecurity policy in moving towards an overall process of creating effective investigators who can effectively counter threats such as ransomware attacks, digital fraud, online exploitation, and cyberterrorism. The study unveils new pedagogies and places significant emphasis on experiential learning models, such as digital forensics simulations, cyber-attack response training, and real-case investigations. The study further explores technology-supported tools that help practitioners develop cutting-edge investigative capabilities, such as virtual laboratories, AI-powered investigation platforms, and blockchain analysis systems. Middle and senior investigator leadership development focuses on decision-making, digital realm ethics, and multidisciplinary investigation team management.

Keywords: *Cybercrime, Investigation, Capacity Building, Education, Cybersecurity.*

INTRODUCTION

The rapid pace of cyber threats calls for innovative learning and capacity-building initiatives to arm investigators with the required competencies in the war against cyber-crime. The more advanced technology becomes, the more cybercriminals devise methods that exploit vulnerabilities in electronic infrastructures, financial networks, and personal data. Cyber-crime, from ransomware to electronic fraud, identity theft, online exploitation, and even cyberterrorism, is among the most serious challenges to international security, economic stability, and personal privacy.

The traditional crime-fighting mechanisms have fallen short as cyber threats have mushroomed in the quest for sophistication. Investigators must be differently equipped with technical, legal, and behavioral competencies to address the challenges of the digital landscape. Training and capacity building in cybercrime investigations are of the highest priority for law enforcement agencies, private security firms, and policy

[1] Dubai Police Academy, Dubai, United Arab Emirates, HABDELRAOUF@dubaipolice.ac.ae

makers seeking to upgrade their capabilities for detection, prevention, and prosecution of cybercriminal activities.

This article therefore reviews some of the transdisciplinary frameworks used in educating professionals to utilize information technology, law, behavioral sciences, and cybersecurity policy. In developing competences for cyber-crime investigators, there is a holistic framework in which such investigators will have skills in digital forensics, cyber threat intelligence, risk management, and ethical hacking. This will make the process easier and enhance responsiveness to evolving threats in cyber-crime investigations, and when necessary, ensuring that experts possess needed competencies.

Also, the research supports the increasing demand for training models that adopt experiential learning, including hands-on training, cyber-attack response drills, and digital forensics simulation. The research also highlights how technology-enabled tools – including virtual labs, AI-driven investigative platforms, and blockchain analytics – will play a major role in investigator preparedness in addressing real challenges.

However, the leadership and ethical dimensions remain critical to decision-making by cyber-crime investigators. Training of mid-level and senior investigators should be directed towards strategic thinking, ethical responsibility, and team leadership to improve the overall performances of cyber-crime investigation units. Inter-cooperation is the basis of cyber-crime training and requires strong academic partnerships with law enforcement, private cybersecurity companies, and international agencies.

This study, therefore, seeks the development of an all-encompassing framework to be applied under sustainable and region-specific capacity building. By aligning global best practices with local legal frameworks and cultural contexts, this study will set cybercrime investigation education as codified in accordance with various regions' needs. Ultimately, the end-product will be about establishing lifelong mechanisms, modular programs, and the international recognition systems for certification where investigators are equipped to address current and future challenges of digital evidence.

Research Objectives

- Discuss the place of transdisciplinary learning in preparing cybercrime investigators.
- Discuss models of experiential learning used in training investigators in investigative techniques.
- Discuss technology-enhanced tools and explore their influence on the investigators' training.
- Discuss leadership and ethics in cyberspace investigations.
- Discuss best practices for collaborative educational courses between academ-

ics, law enforcers, and private cybersecurity firms.

- Propose a country-specific, sustainable framework for capacity-building programs.

LITERATURE REVIEW

The rapid development of cyber threats calls for paradigm-shifting education and innovative capacity-building initiatives in cybercrime investigation. This literature review discusses the potential application of transdisciplinary paradigms to enhance the training and preparation of professionals to cope with the modern intricacies of cybercrime. This review synthesizes insights from various fields, including information technology, law, behavioral sciences, and cybersecurity policy, to advance a comprehensive strategy for the development of effective investigators.

Theoretical Underpinnings of Cyber-Crime Investigation Training

Several theoretical models serve as the foundation for cybercrime investigation training. Routine Activity Theory (RAT) and General Deterrence Theory (GDT) underscore the importance of strategic intervention via training. Training investigations show that educating law enforcement officers with upgraded knowledge in cybercrime investigation can improve the detection, analysis, and prevention of cyber threats (Smith et al., 2020).

Transdisciplinary approaches emphasize the integration of various disciplines such as criminology, computer science, psychology, and digital forensics to provide comprehensive training (Elshenraky, 2024). Constructivist learning models suggest that hands-on, experiential learning is a primary component of training cybercrime investigators (Davis & Brown, 2021). Problem-based learning (PBL) approaches have also been identified as useful means of developing analytical thinking and practical skills for cyber investigations (Liu et al., 2022). In addition, Kolb's experiential learning model holds that situation-based training in real-life situations is a necessity for effective cybercrime investigation training (Williams, 2023).

Cyber-Crime Investigation Training Programs

Literature highlights the importance of structured training programs for cybercrime investigation. Universities and police departments offer specialized courses in digital forensics, basic cybersecurity, and ethical hacking (Jones & Patel, 2021). Online learning websites such as Coursera and edX have also introduced investigator-specific training modules, offering greater flexibility and convenience (Anderson, 2022).

Studies indicate that simulation-based training programs significantly enhance investigative skills. Cyber ranges, which provide real-time controlled environments to conduct cyber-attack investigations, have been recognized as effective capacity-building tools (Wang & Smith, 2023). Technology-savvy tools such as virtual labs, artificial intelligence-supported investigative platforms, and blockchain analysis have served as an important means of delivering hands-on experience (Elshenraky, 2024). Furthermore, gamification techniques have been integrated in cyber-crime training programs to increase learner motivation and skill retention (Johnson & Kim, 2023).

Challenges in Capacity Building for Cyber-Crime Investigation

Another major challenge is the rapid evolution of cybercrime tactics, which continues to outpace traditional investigation training. Cybercriminals continuously develop new attack vectors, exploiting emerging technologies such as artificial intelligence and blockchain to support illicit activities (Smith & Taylor, 2022). Investigators require continuous professional development as well as access to real-time intelligence-sharing forums to stay ahead of such threats. However, many countries lack the infrastructure to provide ongoing specialist training, resulting in law enforcement agencies fall behind.

Besides, resource constraints in developing nations hinder access to advanced forensic software and digital evidence analysis systems. The majority of cybercrime cases require specialized software and hardware to follow and examine cybercriminal activity effectively (Gonzalez, 2023). The high cost of these tools, coupled with minimal government investment in cybersecurity initiatives, restricts investigative capabilities. With insufficient investment in digital forensics laboratories and training programs, most law enforcement agencies are ill-equipped to handle complex cybercrime cases.

Cross-sector cooperation between law enforcement, private industry, and academia is also required but lacking. Successful cybercrime investigations require partnerships across sectors, allowing for knowledge and skills transfer (Harrison et al., 2024). However, bureaucratic processes, data privacy concerns, and jurisdictional disagreements tend to hinder such cooperation. Without effective cross-sector coordination, investigative units cannot leverage the skills and resources necessary to counter sophisticated cyber threats.

Another pressing issue is the shortage of specialized experts with interdisciplinary expertise. Cyber-crime investigation demands experience in computer science, digital forensics, legal systems, and criminology (Patel & Johnson, 2023). However, traditional law enforcement training does not integrate these disciplines, and investigators do not have technical and legal expertise. The lack of university courses or certification programs that fully address cyber-crime investigation further exacerbates this issue, such that it becomes hard to develop a pool of workers with the ability to deal with digital crimes' sophistication.

In addition, cultural and linguistic differences pose hurdles to international cybercrime investigations. Cybercriminals often carry out their operations across borders, taking advantage of differences in national laws and enforcement capabilities to evade prosecution (Nguyen & Park, 2024). Investigation agencies often have difficulty securing the cooperation of foreign governments, especially in nations with weak cybersecurity legislation. Language barriers and varying degrees of technological adoption also hinder cross-border investigations, underscoring the need for more streamlined international coordination frameworks and multilingual training programs.

Best Practices in Cyber-Crime Investigation Education

To improve capacity building, a few best practices have been identified. Partnerships between academic institutions and law enforcement agencies enhance practical training (Smith et al., 2022). Simulation and experiential learning, such as computer forensics laboratories and virtual cyber-crime investigations, increase skill acquisition (Jones, 2021). AI-based training programs adapt instruction to individual student needs, ensuring the acquisition of up-to-date knowledge (Wilson, 2023). Policymakers and governments need to incorporate standardized protocols for training to deliver consistency across all jurisdictions (Miller & Johnson, 2020).

Interdisciplinary approaches are recommended, bringing together psychology, law, and information technology to prepare well-rounded investigators (Morgan et al., 2023). Mentorship and apprenticeship models have also been shown to be successful in knowledge transmission to novice investigators (Taylor, 2023). Region-specific programs designed to work within the relevant legal framework as well as local cultural sensibilities have also been identified as critical components to an effective training program (Elshenraky, 2024).

Additionally, models of lifelong learning and continuous professional development (CPD) have been highlighted as essential for keeping pace with changing cyber threats. Micro-credentialing and stackable certification programs have been used by several organizations to ensure cyber investigators get an opportunity to refresh their skills from time to time (Reed et al., 2023).

1. Public-Private Partnerships for Resource Sharing

Encouraging collaborations between law enforcement, cybersecurity firms, and universities can expose investigators to cutting-edge tools and experts (Davidson & Clark, 2023). Private sector organizations produce advanced cyber defense technologies that can be integrated into law enforcement training programs. Through formal collaborations, investigators gain experience working with real-world cyber threats and forensic equipment that may not be funded by government programs. These collaborations also facilitate the sharing of intelligence, which enables a more proactive approach to threat prevention.

2. Gamification and Immersive Learning Environments

The use of gamification techniques, such as cybersecurity exercises and virtual attack simulations, has proven useful in engaging trainees and increasing retention of investigative technique (Harrison & Lee, 2022). Cyber ranges are tools that allow participants to engage in live cybercrime investigations in a virtual setting, improving their problem-solving skills and responses to emerging threats. Research shows that incorporating game-like elements into training increases motivation and knowledge retention compared to traditional lecture-based methods.

3. Cross-Border Training and International Cooperation Programs

Since cybercrime is a global issue, international training programs help bridge jurisdictional gaps and foster collaboration between law enforcement agencies across the world (Nguyen & Park, 2024). The initiatives aim to harmonize legal frameworks, improving mutual legal assistance treaties (MLATs), and establishing common investigative methods. INTERPOL and Europol have been at the forefront of efforts that train investigators to handle cross-border cases of cybercrime, offering better coordination in tracing and prosecuting cybercriminals.

4. AI-Driven Predictive Analytics for Investigator Training

Artificial intelligence technologies are used to create adaptive training programs that adjust to evolving needs of cybercrime investigators (Wilson, 2023). By analyzing new cyber threats, machine learning algorithms can dynamically update training curricula in real time, keeping investigators informed about new attack techniques. AI-powered assessment platforms also personalize learning experiences, identifying gaps in trainees' skill sets and recommending targeted learning modules for remediation.

5. Ethical and Legal Training for Investigators

Because of the complexity of cybercrime investigations, ethical and legal training should be incorporated into cybercrime education courses (Martinez & Howard, 2023). Investigators must be taught about data privacy laws, digital rights, and ethical considerations when handling digital evidence. Failure to adhere to legal protocols can result in cases being dropped in court due to evidence that was not properly collected or handled. Cyber ethics and compliance training ensures that the investigators remain within the boundaries of the law while upholding human rights and privacy laws.

6. Real-Time Threat Intelligence Integration

Incorporating live threat feeds into training programs keeps investigators up to date with the latest cyber threats and attack vectors (Singh et al., 2024). Cybercrime evolves rapidly, and static training programs become outdated very quickly. Training programs can be adapted in real time to reflect the latest trends in cybercrime using live feeds from cybersecurity firms, government organizations, and industry reports. This approach helps investigators acquire the skills needed to detect, analyze, and respond effectively to emerging threats.

The Role of Technology in Capacity Building

The application of cutting-edge technology in training and education for cybercrime investigation is a new trend. Forensic software based on AI enables faster and more accurate threat analysis (Williams, 2024). Machine learning algorithms are increasingly being utilized to detect cyber threats and predict criminal behavior (Patterson & Green, 2023). Blockchain analytics tools are helping investigators trace illicit transactions, particularly in cryptocurrency-related crimes (Carter, 2023). Virtual and augmented reality (VR/AR) technologies are also utilized to examine immersive cybercrime investigation training (Daniels, 2023).

Cloud computing has also emerged as an essential tool in cybercrime investigation training. Cloud platforms allow investigators to access, store, and analyze vast amounts of digital evidence securely from remote locations (Nguyen & Harris, 2023). Cloud platforms make it possible for collaborative investigations with the capability of sharing case details in real-time between various agencies, thus maximizing coordination in handling cyber threats. Moreover, cloud-based training facilities provide scalable, cost-effective solutions for law enforcement agencies, ensuring that investigators can make use of the latest forensic tools and cybersecurity paradigms without having to build large-scale on-premises infrastructure.

Big data analytics is another revolutionary technology in capacity building. Computer crime investigations gather vast amounts of structured and unstructured information through logs, net flows, and electronic communications (Chen et al., 2024). Advanced data analytics tools aid investigators in analyzing and connecting this data to identify trends, discover deviations, and uncover hidden links to criminal activity. Through the application of big data methods, law enforcement authorities can better monitor cybercrime networks, anticipate future threats, and react more effectively to cybercrimes.

Furthermore, automated incident response systems are streamlining cybercrime investigations by reducing response time and manual effort. Such systems utilize artificial intelligence to process security incidents, prioritize tips, and even automate preprogrammed response procedures (Thompson & Lee, 2023). By incorporating automation into training programs, investigators can acquire skills to effectively address high-volume cyber threats. The use of such systems not only enhances investigative efficiency but also reinforces the fact that cybercrime training remains current in an era where attackers are using more advanced tactics.

Future Directions

Emerging technologies such as artificial intelligence, blockchain, and big data analytics will play a crucial role in the future of cyber-crime investigations. Incorporating these advancements into educational curricula will enhance the preparedness of cybercrime investigators. Additionally, global collaborations will be essential for the development of standardized training programs that address the transnational nature of cyber-crime.

Modular training and certification programs specializing in cybercrime investigation will provide lifelong learning mechanisms, ensuring that investigators remain equipped with up-to-date knowledge and skills (Mitchell & Carter, 2024). Expanding public-private partnerships will also be vital in ensuring up-to-date, practical knowledge in cyber-crime investigations (Rodriguez, 2023). Knowledge exchange through international platforms will further enhance capacity-building efforts by enabling cross-border cooperation (Elshenraky, 2024).

Additionally, the rise of quantum computing poses both challenges and opportunities for cybercrime investigations. The future of digital forensics will likely involve post-quantum cryptography training and the integration of quantum-resistant security measures in law enforcement investigations (Stevenson, 2024).

Education and capacity building in cyber-crime investigations remain critical in combating the growing threat of cyber offenses. While significant progress has been made, challenges such as resource limitations, evolving threats, and legal complexities must be addressed. Strengthening interdisciplinary education, fostering industry collaborations, and leveraging emerging technologies will enhance investigative capabilities in the digital age. A transdisciplinary, technology-enhanced, and globally cooperative approach is necessary to prepare investigators to tackle both current and future digital challenges effectively.

Furthermore, future research should explore how adaptive learning technologies, AI-driven analytics, and international policy harmonization can enhance cybercrime investigation education. By adopting innovative pedagogical strategies and leveraging emerging technologies, institutions can equip investigators with the tools needed to stay ahead of cyber threats in an increasingly digital world.

METHODOLOGY

This study employs a mixed-methods approach, integrating both qualitative and quantitative research methodologies. This approach allows for a comprehensive understanding of the effectiveness of cyber-crime education and capacity-building programs.

Data were collected through surveys and interviews with cybersecurity professionals, law enforcement personnel, and educators involved in cyber-crime investigation training. The surveys yielded quantitative insights into the effectiveness of training programs, while the interviews provided in-depth qualitative perspectives on challenges and best practices.

The research includes case studies of cyber-crime education models from various countries. These case studies provide comparative insights into different approaches and identify the key factors contributing to successful training initiatives.

A comparative analysis was conducted to evaluate various cyber-crime training programs worldwide. This analysis identifies best practices, highlights gaps in current education models, and proposes recommendations for improvements based on successful frameworks.

A thematic analysis was performed to identify key themes in cyber-crime investigation training and capacity building. Themes include the role of interdisciplinary education, the integration of technology, collaboration between public and private sectors, and strategies for lifelong learning.

DISCUSSION

The findings of this study highlight the importance of an interdisciplinary approach to cyber-crime investigation education. The integration of information technology, law, and behavioral sciences ensures a comprehensive understanding of cyber threats. The research confirms that experiential learning methods, such as simulations and real-world case studies, significantly enhance investigators' competencies.

One of the key insights derived from the data is the lack of standardization among existing training programs across regions. This inconsistency hampers collaboration and information sharing among law enforcement agencies globally. The comparative analysis suggests that best practices from successful programs, including the use of cyber ranges and AI-driven investigative tools, should be adopted widely.

Challenges such as financial constraints, evolving cyber threats, and gaps in leadership training were also emphasized. Addressing these issues requires continued collaboration between academia, law enforcement, and private industry. The study further suggests that modular training and lifelong learning frameworks can help practitioners stay updated with emerging cyber threats.

Ultimately, the research underscores the necessity of ongoing investment in cyber-crime education and capacity-building initiatives. By leveraging technology, fostering interdisciplinary collaboration, and implementing best practices, cyber-crime investigators can be better equipped to handle evolving digital threats effectively.

CONCLUSION

Education and capacity building in cyber-crime investigations remain critical in combating the growing threat of cyber offenses. This study has demonstrated the importance of interdisciplinary training, hands-on learning, and technological integration in developing skilled investigators. While challenges such as financial constraints, evolving cyber threats, and leadership gaps persist, adopting best practices and fostering collaborations between academia, law enforcement, and industry can bridge these gaps. Standardized training programs, continuous professional development, and innovative educational frameworks are necessary to equip cyber-crime investigators with the skills required to address current and future digital challenges. Future research should focus on assessing the long-term impact of emerging training methodologies and refining educational models to keep pace with the ever-evolving cyber landscape.

RECOMMENDATIONS

Cyber-crime investigation programs should integrate law, criminology, information technology, and behavioral sciences to provide a holistic education. Curricula must be tailored to address local legal frameworks and socio-cultural factors while aligning with global best practices. Additionally, lifelong learning models, including certification programs and micro-credentialing, should be implemented to keep investigators up to date with emerging threats.

Law enforcement agencies and academic institutions should adopt cyber ranges, AI-driven forensic simulations, and emerging technologies such as AI, blockchain analytics, and VR/AR to enhance hands-on training. Specialized training modules should also focus on decision-making, ethical considerations, and multidisciplinary team management to prepare investigators for the real-world challenges.

Strengthening partnerships between law enforcement, academia, and cybersecurity firms is crucial for knowledge exchange and practical training. Governments should work with international bodies to establish standardized, adaptable training frameworks and encourage participation in global cybersecurity forums, workshops, and research collaborations. Securing investment from both governmental and private sectors is essential for supporting advanced training infrastructure and ongoing research initiatives.

REFERENCE LIST

Ali, M., & Khan, R. (2019). Challenges in Cyber-Crime Investigation Training. *Journal of Cybersecurity Research*, 12(3), 45-58.

Anderson, T. (2022). Online Learning for Cybercrime Investigators. *Educational Technology Review*, 17(1), 34-50.

Brown, K., & White, P. (2021). The Future of Cybercrime Training. *Digital Security Review,* 19(4), 90-104.

Carter, J. (2023). Blockchain Analytics in Criminal Investigations. *Journal of Forensic Studies*, 25(2), 78-89.

Chen, Y., Patel, R., & Kim, S. (2024). Big Data Analytics in Cybercrime Investigations: Enhancing Digital Evidence Processing. *Journal of Cybersecurity Intelligence*, 21(1), 55-72.

Davidson, R., & Clark, J. (2023). Leveraging Public-Private Partnerships in Cybersecurity Training. *Journal of Cybersecurity Policy*, 18(2), 45-67.

Daniels, M. (2023). The Use of VR and AR in Cybercrime Investigation Training: A New Frontier. *International Journal of Digital Forensics*, 19(3), 88-105.

Davies, R., et al. (2023). Global Variations in Cybercrime Training. *International Law and Cybersecurit*y, 14(5), 112-130.

Elshenraky, H. (2024). Transdisciplinary Cybercrime Training Models. *Cybercrime Education Journal*, 22(1), 1-19.

Elshenraky, M. (2024). Leadership Development in Cybercrime Investigation: Bridging the Mid-Career Training Gap. *Digital Forensics Journal*, 22(1), 55-78.

Fischer, L. (2022). Industry Partnerships in Cybercrime Education. *Law Enforcement Training Review*, 20(3), 55-70.

Gonzalez, R. (2023). The Role of Digital Forensic Tools in Modern Cybercrime Investigations. *Journal of Digital Evidence*, 19(4), 88-105.

Harrison, P., Lee, A., & Carter, J. (2024). Enhancing Law Enforcement-Private Sector Collaboration in Cybersecurity Investigations. *Cybersecurity & Policy Review*, 21(2), 63-85.

Harrison, P., & Lee, A. (2022). Gamification in Cybercrime Investigation Education: Enhancing Engagement and Retention. *Cyber Training Review*, 20(1), 78-99.

Johnson, P., & Kim, S. (2023). Gamification in Cybersecurity Education. *Cyber Training Journal*, 16(2), 98-112.

Lee, M. (2020). Keeping Up with Cyber Threats. *Journal of Digital Forensics*, 13(1), 23-36.

Lee, M. (2020). The Evolving Threat Landscape: Why Cybercrime Training Struggles to Keep Up. *Journal of Cyber Threat Analysis,* 11(3), 98-115.

Martinez, L., & Howard, K. (2023). Ethical Considerations in Digital Investigations: Balancing Security and Privacy. *Journal of Cyber Law & Ethics,* 12(4), 115-132.

Miller, D., & Johnson, L. (2020). Standardizing Cybercrime Training. *Cybersecurity Policy Journal*, 10(4), 66-81.

Nguyen, H., & Harris, J. (2023). Cloud Computing and Collaborative Cybercrime Investigations: Overcoming Geographical Barriers. *Cybercrime Review*, 17(2), 34-51.

Nguyen, H., & Park, S. (2024). Overcoming International Barriers in Cybercrime Investigations: A Legal and Linguistic Perspective. *Global Cybersecurity Journal*, 16(1), 39-59.

Nguyen, H., & Park, S. (2024). Strengthening International Cooperation in Cybercrime Training. *Global Cybersecurity Journal*, 16(1), 62-80.

Patel, R., & Johnson, K. (2023). Bridging the Skills Gap in Cybercrime Investigation: The Need for Interdisciplinary Expertise. *Cyber Training Review*, 20(2), 75-92.

Patterson, L., & Green, D. (2023). Machine Learning Applications in Cyber Threat Detection and Criminal Behaviour Prediction. *Journal of AI & Security Studies*, 16(4), 101-120.

Reed, S., et al. (2023). Micro-Credentialing in Law Enforcement. Professional *Development in Cybersecurity*, 21(2), 77-93.

Singh, R., Patel, M., & Kim, S. (2024). The Role of Real-Time Threat Intelligence in Cybercrime Training Programs. *International Journal of Cyber Forensics,* 19(2), 50-73.

Smith, J., & Taylor, B. (2022). The Role of AI and Blockchain in Modern Cybercrime Tactics. *Emerging Tech & Security Journal*, 15(4), 102-125.

Smith, J., et al. (2020). Strategic Interventions in Cybercrime Education. *Criminal Justice & Cybersecurity*, 18(3), 102-115.

Thompson, B., & Lee, A. (2023). Automated Incident Response Systems: Transforming Cybercrime Investigation Efficiency. *Cyber Threat Journal*, 22(1), 44-68.

Williams, H. (2024). AI in Cybercrime Investigations. *Journal of Emerging Technologies*, 27(1), 50-67.

Williams, T. (2024). AI-Powered Forensic Tools: Enhancing Digital Evidence Analysis and Cyber Threat Detection. *Journal of Digital Law Enforcement*, 23(2), 92-110.

Wilson, T. (2023). Artificial Intelligence and Adaptive Learning in Cybercrime Investigation Training. *Journal of Emerging Technologies in Law Enforcement*, 14(3), 88-105.

Katarina Šmakić[1]

THE NECESSITY OF INTEGRATING PHILOSOPHY OF MEDIA INTO THE SECURITY STUDIES' CURRICULUM

Abstract

Transdisciplinarity has become a key direction in scientific thinking because, methodologically speaking, contemporary understanding of the world is so fragmented that it is nearly impossible to reconstruct the whole from it. The narrow specialization of knowledge has led modern science to a form of absurdity, where we are unable to see the broader picture. The main paradox of this "progression" of scientific knowledge is that narrow specialization creates expertise that loses its scientific dimension, or its meaning connected to understanding both the whole and its parts. The primary goal of transdisciplinarity today is to bridge the gap between science and narrowly specialized knowledge, i.e., between science and expertise, in favor of a scientific approach. Philosophy of Media allows for the analysis of the role of media in creating narratives about security, shaping societal attitudes toward risks, and manipulating information, which is crucial in the context of contemporary digital security challenges. By connecting philosophical media theories with security studies, we explore how media not only transmit information but also influence public awareness, political decision-making, and the creation of strategies for dealing with threats. This paper explores the discipline of Philosophy of Media in the context of the transdisciplinarity of security studies, analyzing how media shape perceptions of risk, power, and narratives about security. By linking media theories and security practices, this paper emphasizes the role of media as a tool and space for forming contemporary security regimes. Transdisciplinarity here means connecting various disciplines – such as philosophy, communication studies, media studies, information technology, and security studies – to better understand the complexity of contemporary security challenges, including digital threats. The primary focus is on integrating the Philosophy of Media subject into the security studies curriculum, with the aim of gaining a deeper understanding of how media influence societal narratives, political decisions, and public awareness of security issues. Philosophy of Media enables the analysis of ethical dilemmas related to the distribution of information, misinformation, and manipulation, which is especially relevant in the context of global threats such as terrorism, cyberattacks, or political instability. Through this subject, students would learn how media content can shape societal attitudes toward risks and threats, enabling them to develop the ability to critically analyze the media sphere and recognize its potential impacts on public opinion.

Keywords: *Transdisciplinarity, Philosophy of Media, Security Studies, Digital Threats, Public Opinion.*

[1] Faculty of Diplomacy and Security, University Union-Nikola Tesla, Belgrade, Serbia, katarinasmakic@gmail.com

Transdisciplinarity has become a key direction in scientific thinking, as, methodologically speaking, contemporary understanding of the world is so fragmented that it is nearly impossible to reconstruct the whole from it. The narrow specialization of knowledge has led modern science to a form of absurdity, where we are no longer capable of seeing the bigger picture. The main paradox of this "progress" in scientific knowledge is that narrow specialization creates expertise that loses its scientific dimension, or its meaning connected to understanding both the whole and its parts. The primary goal of transdisciplinarity today is to overcome the gap between science and narrowly specialized knowledge, or between science and expertise, in favor of a scientific approach that allows for the synthesis of different disciplines and perspectives. The history of technological advancement, from the perspective of philosophy, provides a profound reflection on how technology has shaped and continues to shape human existence, knowledge, and society. Various philosophical traditions have engaged with the implications of technological development, often questioning the meaning, ethics, and future of technological progress. With the Industrial Revolution, technological advancement accelerated, and philosophers began to grapple with its social and ethical implications. Karl Marx viewed technology as a force of production that fundamentally shapes class structures and economic systems. For Marx, technological advancements in industry were crucial in shaping the material base of society and thus influencing the superstructure, which includes law, politics, and culture. However, Marx was also critical of the alienation caused by industrial technology, where workers became disconnected from the products of their labor.

Friedrich Nietzsche (Nietzsche, 2009:25) in his critique of modernity, viewed technology with skepticism, fearing that technological advancements could exacerbate the decline of traditional values, leading to what he called the "last man", a figure who has become complacent and devoid of higher purpose due to the comforts of technological society.

> Modern science was born through a violent break with the ancient vision of the world. It was founded on the idea – surprising and revolutionary for that era – of a total separation between the knowing subject and Reality, which was assumed to be completely independent from the subject who observed it. This break allowed science to develop independently of theology, philosophy, and culture. It was a positive act of freedom. But today, the extreme consequences of this break, incarnated by the ideology of scientism, pose the potential danger of self-destruction of our species. (Nicolescu, 2010:21)

The development of science and technology, although undeniably leading to tremendous progress in various fields, has simultaneously produced a tendency toward the fragmentation of knowledge. This fragmentation results in individual research, while methodologically precise and highly specialized, often lacking a broader social and philosophical context, making it difficult to understand their true significance and impact. The rise of digital media and the internet has further amplified the fragmentation of knowledge. The internet provides access to a vast amount of information, but this information is often scattered across various platforms, formats, and languages, creating information overload. The role of search engines, social media, and algorithmic filters has changed how we access, curate, and understand knowledge. As knowledge becomes more fragmented on the internet, people may face difficulty in discerning reliable sources or synthesizing information across different fields. Search engines often present fragmented views, shaped by algorithms that prioritize popular or emotionally engaging content over authoritative knowledge, leading to confirmation bias. This reinforces echo chambers, where individuals are exposed only to information that aligns with their existing beliefs, further dividing knowledge into isolated, often contradictory silos. The digital age is undoubtedly a time of profound epistemic transformation, where the nature of truth, knowledge, and authority is being questioned, redefined, and reshaped. As digital platforms continue to develop, philosophical reflections on the fragmentation of knowledge will remain essential in understanding how human society navigates the challenges and opportunities presented by new technologies.

In this regard, transdisciplinarity does not merely imply cooperation between different disciplines, but also a deeper integration of knowledge that transcends the boundaries of individual scientific areas. This approach not only enables a better understanding of complex phenomena but also fosters the development of innovative methods and theoretical frameworks that can contribute to solving contemporary problems. In fields such as social sciences, philosophy, media studies, information technologies, and security studies, a transdisciplinary approach allows for the examination of phenomena from multiple perspectives, considering their technical, social, ethical, and political dimensions.

Contemporary challenges such as climate change, digital transformation, global security threats, and the impact of media on society cannot be fully understood within the framework of a single discipline. It is necessary to develop research methods that combine quantitative and qualitative analyses, theoretical and empirical research, as well as interdisciplinary strategies that enable a holistic approach to knowledge. In this context, transdisciplinarity not only contributes to the academic community but also becomes crucial for shaping policies, decision-making, and the development of social strategies based on a comprehensive understanding of contemporary problems. Transdisciplinarity is not just a methodological tool, but also a philosophical principle that involves questioning the fundamental assumptions about the nature of knowledge and its role in society. The introduction of a transdisciplinary approach into educational systems can contribute to the formation of generations of researchers and professionals who are capable of connecting different fields of knowledge, critically analyzing information, and developing creative solutions for the complex problems faced by the modern world. In this context, transdisciplinarity involves connecting various disciplines – such as philosophy, communication studies, media studies, information technologies, and security studies – to better understand the complexity of contemporary security challenges, including digital threats.

Media have become an all-encompassing practice that permeates every aspect of life – they are a network, they are the digital world we live in, fast, cheap, political, cultural, economic, and social. Social networks and interconnectedness shape the everyday lives of billions of people around the world. However, much like with social revolutions, those living in an era of media transformation often fail to realize the extent of the radical changes they are undergoing. It is difficult to achieve critical distance when nearly every segment of life is digitally mediated, and unlike in earlier times when historiography provided a narrative sense to changes, today, reflection on media processes becomes increasingly challenging, so „media is now. But like the process of social revolution, to live mediation, to be in the middle of it and to be part of it, is often to not realize that one is partaking in radical social upheaval and technological transformation" (Hassan&Sutherland, 2017:1).

The primary focus is on integrating the subject of Philosophy of Media into the curriculum of security studies, with the aim of deepening the understanding of how the media influence societal narratives, political decisions, and public awareness of security issues. Philosophy of Media enables the analysis of ethical dilemmas related to the distribution of information, misinformation, and manipulation, which is especially relevant in the context of global threats such as terrorism, cyberattacks, or political instability. Through this subject, students would learn how media content can shape societal attitudes toward risks and threats, developing the ability to critically analyze the media sphere and recognize its potential impacts on public opinion, because „as soon as we realise that there are no contents outside the media we have to accept that research in media has to invest deliberately all possibilities of observation and description offered by all media" (Schmidt, 2008:103). Understanding the media as an inseparable part of social reality enables students to develop a critical attitude toward their impact on public opinion. Philosophy of Media, through an interdisciplinary approach, provides key tools for the analysis and reflection on the role of the media in shaping perception, values, and social relationships, possible phenomena, and consequences, thereby contributing to more responsible and conscious use of media content.

Philosophy of Media, as an interdisciplinary field, studies the fundamental ontological, epistemological, and ethical dimensions of the media, analyzing their impact on society, culture, and human perception of reality, the interconnection between different disciplines, the phenomena that arise, and their influence on social relationships.

> In an era (over)emphasizing the end of history, spirit, and in general – metaphysics and its 'narratives' in the age of quantum physics, nanotechnology, neurophysiology, and so-called 'transhumanist' values, knowledge, and skills, which

> are primarily correlated with the needs of the neoliberal market economy, as well as the media world, the question of the need for philosophy and its 'benefits' for human life, as well as for the (philosophical) being itself, is raised again. (Vuksanović, 2017:12)

In the context of the security sector, the media function as a tool of control and power, shaping narratives about threats, war, terrorism, and security. Emphasizing the importance of ideology, Foucault argues that „a stupid despot may constrain his slaves with iron chains; but a true politician binds them even more strongly by the chain of their own ideas; it is at the stable point of reason that he secures the end of the chain; this link is all the stronger in that we do not know of what it is made and we believe it to be our own work“ (Foucault, 1977:102-103).

Šušnjić, in his book *Ribari ljudskih duša*, emphasizes that society has various methods for controlling the behavior of its members and maintaining "order and peace". The first means is physical power, or the power of coercion, which involves the use of force to make members of society comply with rules. However, this method is ineffective because, although it can break physical resistance, it does not lead to the creation of responsibility. Those subjected to violence often perceive it as unjust and seek to change their situation, disregarding the means they use. Additionally, those who exercise violence constantly feel threatened by those they coerce. Prisons, for example, breed hatred rather than real change, and it was believed that the proper path to raising human awareness should be through wisdom and truth, not physical punishment.

The second method, which is more effective than physical force, is the power of rewarding. Rewarding positive behavior creates gratitude, responsibility, and long-term loyalty to those who rewarded the individual. Balzac points out that power seeks to maintain itself by rewarding those who can become its defenders, thus preventing possible revolutions. This method creates stability and loyalty in society.

The third method of controlling behavior is the use of social norms, whether in the form of laws (legal norms), moral norms, religious commandments, ideological guidelines, or customary norms. These norms become internalized over time, meaning that people adopt these norms as part of their everyday life and behavior, regardless of the presence of authorities controlling them. Internalization does not mean the disappearance of control, but rather its transfer from the external world to the individual's inner consciousness. Through this process, control becomes less visible but no less effective. Even though people are not always aware of external control, they still act according to norms that have become part of their beliefs and everyday practices (Šušnjić, 1976:27-28). Essentially, society uses physical coercion, rewarding, and social norms as means to shape the behavior of its members, and the most effective method is when these norms become internally accepted and part of individual consciousness.

The security sector uses the media for propaganda, psychological operations, and disinformation, with Baudrillard (1991) emphasizing that the media does not reflect reality but creates hyperreality, which is particularly significant for war and security narratives. Crisis is a key concept for power in this process, because it is no longer a real phenomenon (e.g., economic or political crisis), but a simulation that creates even greater instability, which actually allows the authorities to remain relevant. Power plays on people's desires, encouraging them to believe that their desires are real and that their fulfillment is possible, even though everything in reality is just a simulation. Baudrillard adds that in a simulated world, where signs and symbols no longer signify anything real, power must rely on the discourse of desire to create the illusion of the existence of goals and true values. Society believes in the simulations of these goals and values because they are accepted as reality, without questioning their authenticity. Baudrillard further develops the idea of hyperreality – a state in which reality has become a simulation, and the simulation has become reality. Hyperreality is a world where everything is hyperreal, and it is no longer possible to separate the real from the false. He argues that the production of the real no longer refers to material products or the economy, but to "the creation of simulations of reality" – society becomes overwhelmed with simulations because an increasing number of "hallucinatory likenesses of the real" are produced.

In this process, all products become mere "simulated products" and even production itself is no longer real. In the end, society becomes overwhelmed with products that hold no true value, as their real reference is lost. Power no longer produces real value but constantly produces and reproduces "illusions" of the real. This illusion is used for manipulation, maintaining the status quo, and controlling the population (Baudrillard, 1991:26). According to Baudrillard, capitalism was the first to initiate the process of destroying the references of reality and redirecting society toward abstract symbols, equivalent signs, which became the essential foundation of capitalist society. It broke down all distinctions between true and false, good and bad, real and unreal, all in the aim of achieving abstract equivalences that allow for easier exchange and control. Through this constant production of illusions, power becomes obsessive and eventually reaches a state of complete hallucination, where the difference between reality and illusion is no longer discernible. This situation encourages society to, alongside the desire for liberation from power, feel nostalgic for the loss of political power and control, which in some cases can lead to reactions such as fascism – an excessive need for a referential sign in a world without reality (Baudrillard, 1991:27).

Security risks associated with the unexamined phenomena arising from digital surveillance, in the context of Baudrillard’s simulation, can seriously jeopardize social, political, and economic security. Data manipulation and privacy violations, as well as algorithmic discrimination, can lead to a breakdown of trust and increased societal polarization. Additionally, the use of surveillance for political purposes, such as election manipulation, threatens democracy and political stability. Furthermore, excessive use of simulations creates an illusion of reality, which diminishes social cohesion and leads to the fragmentation of society, making it vulnerable to conflicts and destabilization. Digital surveillance and information security raise questions about ethics and privacy, while Stiegler points out how technological media shape human memory and experience, which includes algorithmic surveillance, big data analysis, and digital forensics, and he notes „today memory is the object of an industrial exploitation that is also a war of speed: from the computer to program industries in general, via the cognitive sciences, the technics of virtual reality and telepresence together with the biotechnologies, from the media event to the event of technicized life, via the interactive event that makes up computer real time, new conditions of event-ization have been put in place that characterize what we have called light-time“ (Stiegler, 1998:276). And also „[...] human contours are ever more legible with facial recognition, data mapping, and other tracking programs. This is an effect of being surrounded. Everything is animated. We now live in a world where objects count themselves and us“ (Swartz et al, 2019:361).

The media and terrorism are inextricably linked, as modern terrorism cannot exist without media spectacularization (Altheide, 2007), which raises the question of whether the media merely report on violence or unconsciously perpetuate it. Altheide argues that media coverage of the "war on terror" from 2002 to 2006 was based on a discourse of fear, in which the U.S. was portrayed as morally superior, while the September 11 attacks were presented as a crisis requiring the sacrifice of privacy in the name of security. Citizens opposing this sacrifice were portrayed as "privacy advocates". The media connected fear with control and surveillance, while enemies were dehumanized and depicted as threats. Bush downplayed the danger of the enemy, while the media supported the moral dichotomy between the U.S. and its enemies, portraying them as evil and immoral (Altheide, 2007:288). In modern information conflicts, digital platforms become a key battlefield, as hybrid warfare combines classical military and media strategies, with Castells (2009) exploring how digital media create a "network society" susceptible to information wars and manipulation, concluding that "power in the network society is communication power" (Castells, 2009:53). As Castells argues, "power in the network society is power of communication" Philosophy of Media examines how media not only transmit information but also shape reality and social relationships.

Philosophy of Media analyzes how digital media, as key instruments in hybrid wars, not only enable manipulation and the spread of information but also how these processes impact the very meaning of truth, morality, and freedom in the digital environment. Through critical reflection, Philosophy of Media can help in understanding the ethical, political, and security implications of communication in the digital age, providing insight into how power in the information society is used and abused.

Due to its transdisciplinarity, the introduction of the course Philosophy of Media into the curriculum of security studies is a good step towards contemplating security phenomena from the sphere of media reality, as this discipline forms the foundation for understanding media as a critical approach to all media theories. It is not only thinking about media but also a theory and practice that examines the social role of media in the modern world. It should also serve as a tool for understanding the ideologies that shape media reality, including transhumanist and informational dangers such as cyber-terrorism (Vuksanović, 2017:39).

In the book *Philosophy of Media 3: Ontology, Aesthetics, Critique,* the author Divna Vuksanović notes that in contemporary society, philosophy is often considered redundant, particularly from critical positions that come from outside of philosophy itself. As Vuksanović notes, according to Adorno, philosophy loses its significance because it is not profitable, and its place in education, science, and everyday life gradually disappears, no longer recognized as "intellectual capital" that meets the needs of the market and capital. As a result, its institutional position in society is not secured. Instead, philosophy becomes part of academic journals, project tasks, or experiments used to refine existing knowledge and launch new ideas, often within already defined paradigms that do not allow for critical examination. Philosophical articles are often reduced to empirical research or analyses, devoid of deeper philosophical reflections. The original philosophical encyclopedias, which addressed key philosophical issues, hardly exist anymore. The question arises whether philosophy needs marketing to better position itself in the knowledge market, implying that knowledge is defined and subject to market exchange, becoming a commodity traded on the global market (Vuksanović, 2017:13-15).

Although the question of the relationship between philosophy and the market remains open, the belief that philosophy will outlast corporate ideology provides a basis for further analysis. Philosophy differs from other disciplines because it continuously reexamines its values and reasons for existence, which allows it to adapt and avoid outdatedness. Through this process of reexamination, philosophy remains relevant and continues to grow, even in the context of global market economies that do not support critical thinking. In the context of Philosophy of Media, ontology, and critique, the media can contribute to shaping the ontological and epistemological foundations of contemporary security theories by acting as intermediaries between social realities and their interpretations. Media not only extract information from the real world, but also present it selectively, thereby shaping the perception of social phenomena such as risks, threats, and power. Through these narratives, they shape the way we understand security. In this process, the media do not merely reflect reality; they actively create meanings and constructs that shape our collective consciousness of the world.

A critical approach to the media enables an understanding of their role in forming and manipulating security narratives. The media are not just neutral channels for transmitting information; they are active agents in creating and shaping narratives about what constitutes a threat and how it can be controlled or eliminated. Through selective representation of information, the choice of narratives, and the portrayal of certain issues as dangers or risks, the media shape social, political, and economic dynamics.

The media, through their influence on public opinion, can create or undermine trust in institutions, form political agendas, and shape societal attitudes toward security and threats. In this process, they can contribute to the legitimization of certain political decisions, control and security policies, or even military interventions, all through the narratives they promote. Through this critical approach, Philosophy of Media helps clarify how the media are used in creating ideological frameworks that support or challenge specific political agendas in the context of global or national security.

Incorporating Philosophy of Media as a subject into the curriculum of security studies is essential for equipping students with the tools to critically examine and understand the intricate relationship between media, society, and technology. Given that media content shapes societal attitudes toward various issues, including risks and threats, it is crucial for students to develop the ability to analyze how media influences public opinion and social behavior. Philosophy of Media offers a comprehensive framework for understanding the materiality, ethics, and cultural implications of media practices, fostering a deeper awareness of the pervasive role of media in shaping our worldview. By studying Philosophy of Media, students can engage with key concepts related to the influence of media on power structures, cultural narratives, and societal transformation, ultimately contributing to a more informed and reflective public. This approach not only enriches their academic development but also prepares them to navigate and critically engage with the media-dominated world they inhabit.

REFERENCE LIST

Altheide, D. L. (2007). The mass media and terrorism. *Discourse & Communication*, 1(3), 287–308. https://doi.org/10.1177/1750481307079207

Baudrillard, J. (1991). *Simulakrumi i simulacija* (F. Filipović, Trans.). Novi Sad: Matica Srpska.

Castells, M. (2009). *Communication power.* Oxford University Press.

Foucault, M. (1977). *Discipline and punish: The birth of the prison*. Pantheon Books.

Hassan, R., & Sutherland, T. (2017). *Philosophy of media: A short history of ideas and innovations from Socrates to social media*. Routledge.

Nicolescu, B. (2010). Methodology of transdisciplinarity – Levels of reality, logic of the included middle and complexity. *Transdisciplinary Journal of Engineering & Science*, 1(1), 19–38.

Nietzsche, F. (2009). *Tako je govorio Zaratustra* (M. Vujčić, Prev.). Despot Infinitus.

Schmidt, S. J. (2008). Media philosophy-A reasonable programme? In H. Hrachovec & A. Pichler (Eds.), *Philosophy of the Information Society: Proceedings of the 30th International Ludwig Wittgenstein-Symposium in Kirchberg*, 2007 (pp. 89–106). Berlin, Boston: De Gruyter.

Stiegler, B. (1998). *Technics and time, 1: The fault of Epimetheus*. Stanford University Press.

Swartz, J., Wasko, J., Marvin, C., Logan, R. K., & Coleman, B. (2019). Philosophy of Technology: Who Is in the Saddle? *Journalism & Mass Communication Quarterly*, 96(2), 351-366. https://doi.org/10.1177/1077699019841380

Šušnjić, D. (1976). *Ribari ljudskih duša: Ideja manipulacije i manipulacija idejama* (4th ed.). Mladost.

***Milica Bošković*[1]**
***Mina Suknović*[2]**
***Nemanja Stevanović*[3]**

EDUCATION, EQUALITY AND DEVELOPMENT[4]

Abstract

In both contemporary and twentieth-century scholarly literature, it is consistently emphasized that two of the fundamental goals of education are the provision of knowledge and skills essential for individuals' participation in social and political life, as well as for their economic advancement. In today's context, education is increasingly recognized as vital for enabling successful social mobility. It is indisputable that the educational process must empower individuals to think critically and to achieve their desired socio-economic goals and status. Although the right to education is enshrined among the fundamental human rights and incorporated into the highest legal instruments of international organizations and national legislations, its realization remains uneven and frequently falls short of the intended standards. Despite global political efforts to ensure equal access to resources, education, and healthcare—irrespective of gender, religion, nationality, or other personal attributes—this objective has yet to be fully achieved in many parts of the world. This paper will explore the significance of the accessibility and level of education within a society, not only for its socio-economic development but also for the promotion of human rights and gender equality. Through the analysis of statistical data related to three key indices—human security, human development, and gender equality—the study will highlight the critical role that high performance across these indicators and their individual parameters plays in fostering the qualitative development of society and ensuring its substantive security.

Keywords: *Education, Equality, Human Security, Development.*

INTRODUCTION

Education has long been regarded as one of the most esteemed pillars of society - a vital system provided by the state for its citizens and a cornerstone of societal progress. In ancient times, the most learned individuals were considered worthy of lead-

[1] Faculty of Diplomacy and Security, University Union-Nikola Tesla, Belgrade, Serbia, milica.boskovic@fdb.edu.rs

[2] Faculty of Diplomacy and Security, University Union - Nikola Tesla, Belgrade, Serbia

[3] Faculty of Diplomacy and Security, University Union - Nikola Tesla, Belgrade, Serbia

[4] The paper was created within the framework of the Erasmus+ project, Project: 101179820 – TRUST – ERASMUS-EDU-2024-CBHE, titled: Triggering Resilience in Up-and-coming Security Threats

ing communities and shaping political agendas. The right to education is also recognized as a fundamental human right, embedded in the most significant international and national legal instruments. This recognition underscores the importance of knowledge and skills for enhancing all other segments of the state and society, as well as for supporting both life and work processes. Scientific advancements and discoveries have driven qualitative leaps in state and societal development - innovations in industry, medicine, physics, and other disciplines have improved public health, enabled the prevention of diseases, fostered economic and technological growth, and introduced new measures for the protection and security of societies and states.

However, despite the central place education holds, both rhetorically and practically, in global and national policies, the realization of its goals appears increasingly complex, less attainable, and still unequally accessible. Rather than being facilitated by new scientific knowledge and pedagogical innovations, access to education, curricular content, and teaching methodology remain hindered by unresolved societal dilemmas. The vast diversity of knowledge and practical research should have served as an undeniable foundation for recognizing human rights, equality, and the well-being of all individuals as universal norms, rather than sporadic examples of good practice. Despite significant scientific achievements, contemporary theoretical frameworks, and normative advances, many societies and states continue to struggle with gender-based disparities in access to education, employment, income, and the inclusion of vulnerable groups in mainstream education, as well as with other forms of social injustice.

In a significant number of countries still governed by autocracy, nepotism, and conformism, many are left questioning whether education is truly worth pursuing. The answer must always be yes. A high level of educational attainment and diversity of knowledge remain key factors in improving individuals' socio-economic status and raising awareness of human rights. When coupled with the realization of other fundamental components - such as access to healthcare and a healthy environment - education contributes to a greater sense of security among individuals and communities, and, by extension, to the overall security of the state. In support of this claim, the present paper examines the relationship between educational attainment and gender equality indices across different countries.

Education – Function and Challenges

In both contemporary and twentieth-century academic literature, two fundamental aims of education are frequently emphasized: first, equipping individuals with knowledge and skills relevant for their future engagement in social, political, and economic life, and second, today more than ever, enabling successful social mobility. Undoubtedly, the educational process should empower individuals for critical thinking and the achievement of desired socio-economic goals and status. In modern societies, the education system is expected to fulfill two widely recognized functions: first, to enrich individuals with knowledge that enables their participation in social, economic, and political life (Durkheim, 1922); and second, to provide access to valuable credentials regardless of one's socio-economic background – in other words, to offer opportunities for social mobility (Labaree, 1997).

The right to education is one of the fundamental human rights. However, although this right is incorporated into the highest international and national legislative frameworks, this does not imply its full realization in practice. Countries that offer equal rights and economic opportunities for men and women rank among the wealthiest in the world (Eastin & Prakash, 2009). In politically and socio-economically developed countries, education is considered the main strategy for achieving sustainable development, due to its capacity to qualitatively and positively transform individual values and behaviors towards more sustainable ways of living and working.

Despite global political efforts to ensure equal access to resources, education, and healthcare for all, regardless of gender, religion, ethnicity, or other personal attributes, this goal remains unattained in many countries. Certain domains are still undergoing processes of adaptation and transformation in accordance with broader social changes. One such area undergoing substantial reform is how equality, diversity, and inclusion are embedded into the ethos of every higher education institution, for the benefit of students, staff, and society as a whole (Carew et al., 2024:26).

Although it may seem surprising that we are still debating the accessibility and benefits of education in the 21st century, it is equally striking that, in some countries, women are still denied the right to education. Even where they do have access, their knowledge and skills are often not equally recognized or economically valued, particularly in terms of career advancement, compared to their male counterparts. Several studies have shown that education in the field of management reinforces gender division by promoting knowledge aligned with values, ideas, and biases that ultimately reflect male dominance in business programs (Hall, 2013; Smith, 2000).

The insistence on gender equality in education and equal opportunities in the labor market is grounded in findings that "gender disparities can have serious economic consequences, as they hinder access to opportunities for women... These disparities tend to be reduced in developed economies" (Sudarso et al., 2019). However, the gap in economic, social, and political participation remains significant in developing countries (Eastin & Prakash, 2009).

Gender inequality in access to and recognition of education is not only a socio-economic issue, but also a security concern. When an entire segment of society - women in this case - is excluded from political and professional processes or even denied the right to participate in state and economic affairs, it reflects the preservation of patriarchal and stereotypical foundations of the state. These structures often serve as a "justification" for domestic violence, sexual harassment, and discrimination. Societies and states in which gender biases and related inequalities, violence, and crimes prevail cannot be considered safe - for either women or men - and other vulnerable groups often suffer similar violations of rights and victimization.

The seriousness of this condition is highlighted by the fact that "vulnerable groups, such as those experiencing helplessness or hopelessness, living in poor socio-economic conditions or coming from dysfunctional family and emotional environments, are easy targets for manipulation and recruitment into human trafficking networks, ultimately becoming victims" (Janković, 2022:95). Education, both formal and informal, understood in its broadest sense, serves as a barrier against societal stagnation and the victimization of already at-risk groups. Without it, the advancement of collective awareness, the rule of law, and overall security and well-being remain unattainable.

Socio-economic well-being, the rule of democracy, a healthy environment, and the respect for human rights have proven to be key pillars of prosperity and social cohesion, and consequently, of both internal and external security (Janković & Bošković, 2024). The principles of equality, diversity, and inclusion are rooted in the civil rights and social justice movements of the 20th century, particularly those of the 1960s, which arose in response to systemic discrimination, marginalization, and segregation (Newman, 2019). Countries that recognized this problem and took active steps to eliminate it are, today, significantly more advanced in terms of security, education, and economic development.

Education, Equality, and Development – A Review of Statistical Indicators

One of the concepts that aptly captures the importance of education, healthcare, and socio-economic policies as pillars of a secure state and society is Human Security. From this overarching theory, other approaches have evolved that regard the individual as the primary referent object of security. Through the integration of research and perspectives, these approaches offer a comprehensive view of the needs that must be met for communities to be secure and capable of sustainable development - such as societal security, environmental security, and economic security.

> With the development of the concept of human security, the need simultaneously arose for constructing a methodological tool that would enable the comparison of human security status at the international level. These efforts resulted in the establishment of the Human Security Index (HSI), with its first version created in 2008 and an improved version released in 2010. (Hastings, 2010)

Hastings' methodology for calculating the Human Security Index defines three categories: 1) Economic Status Index 2) Environmental Status Index 3) Social Status Index. Each of these categories involves the measurement of several parameters, including:

1) Economic Status Index:
    a) Gross Domestic Product (GDP) per capita
    b) Income equality (Gini coefficient)
    c) External debt (as a percentage of GDP)
2) Environmental Status Index:
    a) Emissions of harmful gases per capita
    b) Environmental vulnerability index
3) Social Status Index:
    a) Literacy rate
    b) Political stability and absence of violence
    c) GDP per capita

The maximum HSI value is 1, and the minimum is 0. In 2010, Hastings analyzed data from 230 countries worldwide, calculated the HSI for each, and ranked and classified states into three categories: 1) Countries with high HSI values 2) Countries with so-called “medium” HSI values 3) Countries with low HSI values.

For the purposes of this study, we will present HSI values alongside updated data from the EUROSTAT database for European countries - a continent to which our country belongs, and whose political and economic structures the Republic of Serbia aspires to join through EU membership.

According to Hastings’ 2010 HSI analysis, the highest-ranked countries in Europe (and globally) included Sweden (HSI 0.911), Finland (HSI 0.908), and Denmark (HSI 0.889). Among the countries classified with “medium” HSI values, the highest-ranked European countries were Cyprus (0.796), the Czech Republic (0.781), and Slovakia (0.764). The lowest-ranked European countries within this category were Albania (0.711), Serbia (0.680), and Turkey (0.654). No European countries fell into the lowest HSI category.

The United Nations Development Programme (UNDP) developed the concept of the Human Development Index (HDI) in 1990, emphasizing that: “Human development is the process of enlarging people's choices. The most critical of these choices are to lead a long and healthy life, to be educated, and to have access to resources needed for a decent standard of living” (UNDP, 2010, p. 12).

The HDI encompasses three key dimensions: 1) Health 2) Education 3) Standard of living. These dimensions are assessed through the following indicators: a) Life expectancy at birth b) Expected years of schooling c) Mean years of schooling d) Gross National Income (GNI) per capita. By synthesizing the values of these parameters, the HDI score is calculated, and countries are ranked accordingly.

In 2010, when the HSI values were also published, UNDP ranked 169 countries based on HDI scores. The European countries mentioned earlier occupied the following positions:

1. Sweden – 9th place
2. Finland – 16th place
3. Denmark – 19th place
4. Cyprus – 35th place
5. Croatia – 51st place
6. Slovakia – 31st place
7. Serbia – 60th place
8. Turkey – 83rd place
9. Albania – 64th place

Among the countries with the lowest HDI values, there were no European states; this category was predominantly comprised of countries from Africa and South America. Since this analysis was conducted in 2010, the following sections will also present updated data covering the last five years for which reports are available (2018–2022), as shown in Table 1. To complement the analysis of the role of education, development, and equality, we will also present the Gender Equality Index for the same period. The Gender Equality Index is based on several parameters analyzed by gender, including: a) Level of educational attainment b) Income disparity c) Share of power, i.e., representation in decision-making positions concerning socio-political and economic processes critical to state and economy functioning.

All these data will be presented for the countries whose HSI and HDI were previously analyzed and that are members of the European Union (as the Gender Equality Index is not calculated for non-EU countries). The rankings for the year 2010 will first be presented, followed by rankings for the last five years (2018–2022) for which official reports have been published.

Table 1. *HDI Values and Country Rankings for the Period 2010 and 2018-2022.*

COUNTRY/YEAR	2010	2018	2019	2020	2021	2022
Sweden	9	7	8	7	7	5
Finland	16	15	12	11	11	12
Denmark	19	11	11	10	6	5
Cyprus	35	32	31	33	29	29
Croatia	51	46	46	43	40	39
Slovakia	31	38	36	39	45	45
Serbia	60	67	63	64	63	65
Turkey	83	64	59	54	48	45
Albania	64	68	69	69	67	74

Source: UNDP

The data presented in Table 1 indicate that countries with the highest Human Security Index (HSI) values in 2010 also occupy some of the top positions according to the Human Development Index (HDI). Furthermore, European Union member states demonstrate an upward trend in HDI values over the five-year period compared to 2010, reflecting improved rankings. Among non-EU countries, only Turkey has recorded progress, while Serbia and Albania have experienced a decline in their rankings relative to 2010.

The Gender Equality Index is monitored and calculated by the European Institute for Gender Equality, an EU body, and unfortunately, it covers only EU member states. Table 2 will present the five-year values of the overall index, as well as selected parameters constituting the index: equality in education, equality in earnings, and equality in power, referring to access to decision-making positions in socio-political and economic spheres. The values will be shown for the reference year 2010, as well as for the period from 2018 to 2022.

Table 2. *Gender Equality Index Values and Selected Parameters for 2010 and the 2018–2022 Period.*

COUNTRY/YEAR PARAMETER/RESULT	2010	2018	2019	2020	2021	2022
Sweden	80.1	83.8	83.9	83.9	82.2	82
Equality in education	70.7	74.2	75.2	74.6	76.4	76.1
Equality in earnings	85.3	86.8	85.4	85.9	87.2	85.7
Equality in power	77.8	84.2	84.5	84.6	85.1	85.8
Finland	73.1	74.7	75.3	75.4	74.4	74.5
Equality in education	58.6	61.6	61.9	61.5	60.5	59.7
Equality in earnings	84.1	87.1	87.9	87.5	87.4	86.7
Equality in power	69.1	71.9	74.3	74.3	73.9	75.8
Denmark	75.2	74.7	77.8	77.8	77.8	78.8
Equality in education	73.2	71.3	71	69.3	69.2	70.2
Equality in earnings	83.6	86.8	89.1	88.5	89.5	89.5
Equality in power	58	66.2	66.8	69.3	73.9	77.7
Cyprus	49	56.9	57	57.3	60.7	60.9
Equality in education	55.5	56.2	56	57.8	65.5	66.1
Equality in earnings	80.7	81.7	82.6	83.1	84.3	84.1
Equality in power	15.4	29.8	30	30.1	29.2	28.8
Croatia	52.3	57.9	59.2	60.7	60.7	59.7
Equality in education	49.9	51.6	51.8	53.4	54.2	53.9
Equality in earnings	68.6	72.6	74	74.1	73.6	74.7
Equality in power	28.4	41.4	45.3	49.7	49.5	44.2
Slovakia	53	55.5	56	56	59.2	59.9
Equality in education	59.5	61.2	61.6	60.9	62.1	66
Equality in earnings	70.2	75.1	75.1	74.8	74.2	74.5
Equality in power	29.5	29.6	30.7	31.4	31.1	30.4

Source: EIGE

The data presented in Table 2 demonstrate that countries consistently occupying top positions on the Human Security Index (HSI) and the Human Development Index (HDI) also achieve the highest scores (ranging from 0 to 100) on the Gender Equality Index - and conversely, lower-ranked countries record lower scores. Although all countries show an overall upward trend in gender equality scores, stagnation or even decline can be observed within individual parameters. It is particularly notable that the highest levels of equality are achieved in earnings parity (i.e., comparable salaries for men and women in equivalent positions). Nevertheless, a decline in one parameter often correlates with declines in others, a trend most visible in countries with comparatively lower overall scores: a drop in educational equality most strongly impacts equality in power, and to a slightly lesser extent, equality in earnings.

While top-performing countries sustain or improve levels of educational equality - and especially equality in power - lower-performing countries have experienced a decline over recent years. In fact, these countries have yet to achieve the widely accepted benchmark of 40% women's participation in legislative and executive branches of government.

Given the previously outlined findings on educational access, sustainability, quality of life, and equality, the relevance of United Nations Security Council Resolution 1325 "Women, Peace and Security" (2000) becomes even more pronounced. As Janković and Bošković (2024, p. 92) observe, it remains "perhaps the most robust and elaborated mechanism for advancing gender equality, empowering women, and integrating them into security structures." Similarly, as Hendricks (2012, p. 11) has emphasized, "the link between gender equality, development, and security is widely acknowledged... yet there remains a significant lack of scientific studies on the subject."

Both scholarly research and practical experience underscore a fundamental reality: there can be no sustainable societal development, citizen well-being, or enduring security without equality and inclusion. However, genuine inclusion presupposes a high level of societal awareness regarding tolerance, diversity, and human rights - an awareness that cannot be cultivated without accessible, high-quality education for all.

CONCLUSION

Although education constitutes a relatively coherent system, it is neither exclusively nor should it be solely concerned with the transmission of knowledge. Rather, it must also fulfill an essential formative role. Without the systematic and coordinated implementation of both educational and socialization processes, it is unrealistic to expect the development of individuals who are capable of rational self-perception, critical reflection, and the balanced fulfillment of both fundamental and broader human needs - without doing so at the expense of others.

Given the pervasive influence of technology and social media - whose often uncontrolled and inappropriate content increasingly permeates the daily lives of both children and adults - the institutional and human resource capacities of education must be significantly strengthened in both scope and quality.

Evidence that even in certain EU member states - despite the EU's foundational commitment to human rights, democracy, and the highest societal values - gender equality remains far from achieved in the realms of education and socio-political participation, reveals the enduring strength of stereotypes and traditional patriarchal values. These values are often misaligned with the principles enshrined in the highest international and national legal instruments, namely the commitment to "equal rights for all," a principle that must transcend rhetorical affirmation and become an operative standard of thought and action.

Without universally accessible education, healthcare, legal protection, and justice, genuine societal advancement cannot occur. In this context, a focus on quantitative growth without ensuring qualitative improvement merely results in the artificial inflation of economic and security indicators, while the benefits of such development remain unequally distributed across society.

Moreover, in such environments, stereotypes often fuel acts of violence and aggression, with perpetrators finding both justification and support within segments of society. If societies aim to move beyond reliance on legislation and repressive measures - which address symptoms rather than underlying causes - then high-quality education, the cultivation of life skills, and the internalization of the principle of the inviolability of human equality must serve as the cornerstone and foundation of sustainable development and collective security.

REFERENCE LIST

Carew, P., J. et al. (2024). From Philosophy to Praxis: A Framework for investigating Equality, Diversity and inclusion Manifestation in Higher Education institutions. *iFAC-PapersOnLine*, Volume 58, issue 3, 26-31

Durkheim, E. (1922). *Education and Sociology.* Free Press, New York.

Eastin, J., Prakash, A. (2009). Economic development and gender equality: is there a gender Kuznets curve?. In: *Paper Presented at the 50th Annual Convention of the international Studies Association*, New York.

Hall, S. (2013). Business education and the (Re)production of gendered cultures of work in the city of london. *Social Politics: international Studies in Gender, State & Society*, 20(2), 222–241. https://academic.oup.com/sp/article-lookup/doi/10.1093/sp/jxt010.

Hastingd, D., A. (2010). *The Human Security index: Pursuing enriched characterization of development*. DOi:10.1057/dev.2013.7

Hendricks, C. (2012). Gender, security and development: United Nations Security Resolution 1325 and the Millennium Development Goals. *Agenda: Empowering Women for Gender Equity*, 26(1 (91)), 11–19. http://www.jstor.org/stable/23287227

Janković, B. (2022). Značaj rodno osetljivog pristupa u borbi protiv trgovine ljudima. *Diplomatija i bezbednost*, Godina 5, broj 2, str. 91-103

Janković, B., & Bošković, M. (2024). Značaj primene Rezolucije SB UN 1325 u ostvarivanju stanja humane bezbednosti. *Srpska politička misao*, 84(2), 87-103.

Labaree, D., F. (1997). Public goods, private goods. The American struggle over educational goals. *Am. Educ. Res. J.* 34, 39–81.

Newman, M. (2019). *The civil rights movement*. Edinburgh University Press

Smith, C. R. (2000). Notes from the field: Gender issues in the management curriculum: A survey of student experiences. *Gender, Work and Organization*, 7(3), 158–167. https://doi.org/10.1111/1468-0432.00104

Sudarso, S., Keban, P.E., Mas'udah, S., 2019. Gender, religion and patriarchy: the educational discrimination of coastal Madurese women, East Java. J. int. *Wom. Stud.* 20 (9), 1–12.

United Nations Development Programme. (2010). *Human Development Report 2010*. New York

***Jasmina Šljivić*[1]**
***Boro Krstić*[2]**
***Ljiljana Tomić*[3]**

TRANSDISCIPLINARITY APPROACH IN HEALTH DATA SECURITY AND PRIVACY

Abstract

The study of human security requires the understanding of issues related to health and personal security. Therefore, it is important to conduct research in complex health system using a modern transdisciplinarity approach based on social determinants, data science and decision-making. The main aim of health information system is to ensure security, privacy, confidentiality, availability and integrity of medical data. Information and communication technologies definitely transformed the concept of providing of healthcare and improved its quality and efficiency. However, smart healthcare has jeopardized security and privacy of medical data which became serious issue, so it was necessary to develop adequate strategies to address these challenges. Regulatory authorities have fundamental impact in the establishment of standards which ensure the efficiency, safety and privacy of smart health technologies. Various different technologies enhance the security and privacy of medical data. Comprehensive literature review and analysis of healthcare data security techniques have significant contribution. There is a highlighted necessity for further identification of potential threats and for solving of new security challenges regarding to secure access control and secure data sharing and storage. Continuous education of healthcare professionals about best practices in this area is of crucial importance.

Keywords: *Transdisciplinarity, Security Study, Privacy, Health Data, Smart Healthcare.*

INTRODUCTION

Security is generally defined as one of the basic human needs which are highlighted by the absence of the risk to lose any goods. Examination of security issues is a complex process which requires obligatory actions in the balance of national and international levels. Security issues are research subject in the cognitive field of numerous scientific disciplines. Different scientific disciplines distinguish security based on the

[1] Faculty of Pharmacy, „Bijeljina“ University, Bijeljina, Bosnia and Herzegovina, jasminasljivic86@gmail.com

[2] Faculty of Pharmacy, „Bijeljina“ University, Bijeljina, Bosnia and Herzegovina, direktor@ubn.rs.ba

[3] Faculty of Pharmacy, „Bijeljina“ University, Bijeljina, Bosnia and Herzegovina, ljiljanatomic1965@gmail.com

terms of its own field research. The overall aim is to present security from different aspects and to generally increase knowledge (Czupryński et al., 2021).

It is possible to distinguish two parallel intersect strands in understanding of health system and the overall health. First strand relates to social and economic factors as social determinants contributing to the populations' health. Personal income, education, sex, ethnicity and environment generally affect health outcomes. The second strand is technology which collects characteristic data about patient's activities context and behavior. Collected data present new opportunities for analysis of health for individuals and population. This approach presents new source of data about patient's health and technologies which improve health outcomes and decision-making process. Big data, artificial intelligence and development of genomics are preconditions for improvements in the health of the population. Understanding of these concepts leads to improved decision-making from local to globe level, so transdisciplinarity becomes inevitable. Data science points to understanding of social determinants of health along with decision-making which definitely improves health of the population. Genomic data are extremely sensitive so it is of crucial importance to ensure security and privacy. Genomic data contain personal information and information about family so security assessments should be continuous (Galea et al., 2020).

TRANSDISCIPLINARY SECURITY RESEARCH

Researches in interdisciplinar, multidisciplinar and transdisciplinar perspective related to the interaction of the research subject and its environment is emphasized. Security systems are defined as open and social systems. Security issues can be distinguished in the aspect of separatization in different fields (economic, social, political, military, and ecological) and in human security which relates to health security, food security and personal security. It is crucial to conduct systematic research with the use of methods, techniques, tools and strategies in interdisciplinar, multidisciplinary and transdisciplinar approach. Transdisciplinarity referes to knowledge results between and above disciplines which are based on the new methodology. Interdisciplinarity and transdisciplinarity research in the field of security must be conducted regarded to the position of the research subject (social, economic, political, military, personal, food, health security). Security sciences imply the protection of human rights, human dignity and proper conditions. Therefore, these studies are on the border between different fields of social, psychological and humanistic knowledge. The main research problem of security sciences is related to the recognition of significant factors which influence security. Defined scope of cognition of security sciences are securitization and human security. On the other hand, main research problem for health sciences encompasses the identification of social aspects of health level and medically based services which relates to the state where human feel safe. The scope of cognition is the influence of social determinants to the level of quality of health security. Security is existential need which ensures overall improvements (Czupryński et al., 2021).

HEALTH INFORMATION SYSTEMS

Electronic health records, health applications, wearables led to formation of large bases of health data. These data are significant in provision of direct care to patient (Yigzaw et al., 2022). Health information system is defined as complex system based on modern technologies with the aim to organize and to manage information and data in healthcare institution. These systems provide safe storage, operative retrieval, comprehensive analysis and the exchange of health information with the aim to provide adequate patient healthcare. The quality of healthcare system is defined by secure, confidential, available and integral medical data. These systems encompass various software solutions for different needs. Digitalization of information in healthcare institutions caused numerous threats for security and privacy of the patient's personal data. Patient medical data relates to extremely sensitive information (health, personal identification, personal life, medical history, diagnoses, and treatments). Therefore, these data are highly vulnerable to breach and can cause medical malpractice, frauds, identity theft, discrimination and other various negative consequences. Health information system must integrate design and implementation of proper privacy and security solutions with the use of appropriate technologies for storage and access to data. Technologies can be observed from aspects of secure data storage, sharing and access control. Secure frameworks, protocols for authentication, infrastructure for privacy preservation, data storage and data access control can be used. Selected technologies differ in their purpose, characteristics, functions, features, operating systems, access interface, risks and countermeasures (Shojaei et al., 2024). Health information and communication technologies impact productivity, clinical quality and costs of provided healthcare (Bronsoler et al., 2022).

Medical data are shared between professionals included in healthcare provision with the aim of ensuring appropriate care for patient. Medical data can also be used for further improvements in the field of medicine and science. Appropriate timely access to medical data improves efficiency of healthcare, minimizes medical errors, and increases satisfaction of the patient by provided service and influences cost-effectiveness (Yigzaw et al., 2022).

MEDICAL DATA SECURITY AND PRIVACY

There are numerous reasons for targeting health data, such as lack of security for storage of these types of data. Fraud accounts, illegal purchase of drug and medical equipment and false medical care were recorded. Usually victims are not aware of these thefts (Shakil et al., 2020). The use of patient's identification data and data related to health increase security and privacy concerns (Yigzaw et al., 2022).

Security of medical data which relates to patient information implies their protection from unauthorized revealing, use and access. Privacy refers to specified security aspects with the aim to navigate the storage and sharing of the private information. Privacy ensures that only patients can manage access and the use of their confidential medical data. Numerous countries developed regulations about these issues. All healthcare providers are obliged to adhere to them. European Medicines Agency and U.S. Food and Drug Administration are fundamental in the establishment of standards which ensure safe, efficient and private technologies with the aim of data protection and system integrity preservation (Shojaei et al., 2024).

Healthcare providers are obliged to the implementation of risk management strategy with the aim to manage risks. The goal is reduction of risk to acceptable level which will preserve system benefits (Yigzaw et al., 2022). Healthcare systems are obliged to maintain security and privacy of medical data by development of adequate strategies guided by crucial goals which relates to authentication, user privacy confidentiality, access control, availability and integrity. Smart healthcare integrates patient and doctor on one shared platform while monitoring is done through activity analysis (Alzu'bi et al., 2024).

CYBERSECURITY IN HEALTHCARE

Cybersecurity is a transdisciplinarity field which ensures medical data safety and privacy. This approach is essential to ensure satisfying cybersecurity at all levels. Transdisciplinarity is actually integration of social, natural and health sciences with technology exceeding their own boundaries (van Drumpt et al., 2024; Ferdousi, 2024).

The most significant concerns related to cybersecurity in healthcare are integrity, confidentiality and data availability. Authenticity, authorization and non-repudiation should also be considered. General data protection regulation defines that health data management is in risk of information confidentiality and unregistered changes in medical records. Medical data availability to authorized parties is of crucial importance. Data breaches decreases quality of provided care leading to unsatisfying treatment. Healthcare providers are exposed to serious incidents. Malicious attacks relate to ransomware, phishing and attack related to social engineering. Phishing is jeopardizing the systems and networks because of exploitation of access. Ransomware relates to sending a malware with the hope that victims would pay. Ransom payment definitely does not guarantee that data would be further used on illegal market. Regular and off-line backup are used for minimization of these incidents. Unintentional loss of medical data on mobile devices is also challenging so adequate encryption should be used. These issues can be prevented by training of healthcare professionals and raising their security awareness (Yigzaw et al., 2022).

MOBILE HEALTH APPLICATIONS

Mobile devices are significant in the management of the medical data. Health institution must undertake adequate measures and ensure privacy and security and to prevent unauthorized access and possible threats. Mobile health applications protect health data from the phase of its collection, over storage, access and transmission. Encryption is definitely significant for medical data protection, so it is important to strongly encrypt channels for communication and the storage of medical data on the device and on the cloud. Numerous mobile health applications have inadequate backup mechanism (Ullah et al., 2021).

Secure framework for collection of data can also be used for the design of mobile health applications with the aim to minimize the risk of unauthorized access which encompass encryption, backup and recovery system, secured data, storage and simple use. This results in safe process for data exchange (Simplicio et al., 2015). Secure cloud storage enables backup and additional security measures (Tong et al., 2014).

Methods which are based on detection of privacy-aware anomalies identify abnormalities and preserve the overall integrity of medical data (Shojaei et al., 2024; Xie et al., 2022).

THE INTERNET OF THINGS (IoT), BLOCKCHAIN AND CLOUD COMPUTING

IoT enables data collection and their exchange by integrating encryption and authentication with the aim to protect medical data (Arul et al., 2024). These devices navigate medical data storage, organization access and analysis (Bigini and Lattanzi, 2022; Ferdousi, 2024). They also reduce cost and show additional benefits. On the other hand, many devices definitely have weak passwords (Elhoseny et al., 2021).

Patient records can be transferred from smart device to cloud computing medium with the aim to analyze them and to store them. Jeopardized data security and privacy is serious challenge for healthcare providers (Ferdousi, 2024). It is of crucial importance to implement measures for data protection and develop security standards and protocols (Kelly et al., 2020; Shojaei et al., 2024).

Internet of medical things devices is consisted of very intelligent equipment (medical or vital surveillance, wearables) for use in healthcare purposes at home or at stationary health institutions. IoT captures medical data and send it to physicians who can be alerted by devices with the aim to minimize security threats. Patient care IoT minimizes the need of clinicians to be present. Blockchain technology can be used by patient with the aim of allowing the partial access to specific health records in defined period. Digital authentication based on blockchain presents the authenticable evaluation of digital identity. The focus of blackchain encryption of data is to ensure the translation of original information to encoded text (Arul et al., 2024).

Blockchain technology is transparent and secure for storage and sharing of medical data and it lacks central authority for data control. Blockchain overcomes numerous challenges regarding to medical data security and privacy, so it is necessary to establish mechanism for protection of medical data. Additional issues relate to technology speed, capacity and scalability and also to the data sharing which can jeopardize security and privacy of sensitive medical data. It enables secure sharing of medical data between those who have authorized access. Consistent permissions are main challenge (Arul et al., 2024; Saini et al., 2021, Sanka and Cheung, 2021). Blockchain applications control patient’s sensitive medical data (Dubovitskaya et al., 2020; Shojaei et al., 2024).

Cloud computing has numerous advantages which ensure secure and private medical data. This technology is characterized by encryption, strong control of access and security level, redundancy and compliance. Robust mechanisms for access control can be implemented. Multi-level authentication and access control which is based on the specific role is used to ensure that exclusively authorized parties have the possibility to access medical data which enhance overall security. Cloud computing improves collaboration and scalability and reduces costs because there is no need for hardware and software, which is significant advantage (Shakil et al., 2020). It is important to emphasize that data recovery is guaranteed by cloud computing (Qiu et al., 2020). Data storage on cloud definitely enhances security and privacy of patient information. However, healthcare institutions hesitate to cloud computing because of its vulnerabilities to data breaches and hacking, which would jeopardize medical information. Security concerns are justified because of remote storage of data, network environment and massive sharing of infrastructure (Mehrtak et al., 2021; Shojaei et al., 2024). The special challenge is to control data and to regulate ownership and data interception (AI-Issa et al., 2019).

Easier collaboration process, significant cost-effectiveness, significantly increased speed, flexibility and scalability are advantages of cloud computing which generally decreases infrastructural and operative costs of healthcare providers. Access to information is significantly speeded up, along with removing the barriers between stakeholders and patients. Confidentiality is obligatory although patients' records need to be available to numerous healthcare professionals. There is a growing need for revision of presented solution and their constant improvements. Comprehensive literature review pointed out that the most important security challenges are confidentiality, security, availability and integrity of data and the security of network. On the other hand, encryption, authentication, program interfaces and classification of data present potential solutions for challenges related to security (Mehrtak et al., 2021).

Records of e-health have exponential growth and they are consisted of text, graphs and images, unstructured, unencrypted and it is not possible to manage these data using traditional system. Management of these data is quite challenging. The situation is even more complex when healthcare institutions have several different branches. Cloud computing is thus rather appropriate solution. Electronic medical records and electronic health records maintain health records and they are extremely vulnerable to numerous security threats from healthcare professionals or hackers. Security approach based on biometry is obtained from confidentiality (measure of the system's ability for protection of stored medical data), integrity (existence and continuous accuracy of medical data), non-repudiation (preservation of medical data authenticity after users' access to them) and authentication (verification of the users' legitimacy). Biometric signature is very significant mechanism for authentication. Combinations of biometrics with cloud can be useful for management of medical records. BAMHealthCloud presents useful example of combination between cloud computing and biometric authentication. The final goal is to increase data processing and to ensure data storage, management, and retrieval as well as secure access (Shakil et al., 2020).

SECURE ACCESS CONTROL

It is possible do distinguish three different security aspects which relates to secure access control, data storage and data sharing which are important for health information system. The most important component of health information system is secure access control which ensures the security and privacy of medical data. This instrumental control regulates access to data and consequently prevents data breaches. The result is efficient reduction of various risks and potential threats. The aim is to ensure that only authorized parties have access to highly sensitive and confident medical data. This approach prevents any unauthorized access and data manipulation. Data breaches definitely cause huge damages to healthcare institutions and significantly increases costs of communication and computationalization. Restrictive and controlled access to data minimizes data breaches and enhances overall security.

Literature review showed that specific systems are efficient for real-time healthcare, while other agent-based systems are suitable for e-health systems. Therefore, it is emphasized that secure access control is of crucial importance for security and privacy of sensitive medical data. Despite all advantages this aspect of security is also characterized by several challenges. Multiple levels of secure access control can be found in health information systems, such as authentication, authorization or audit logging. These systems are rather complex for management and configuration. It is often necessary to integrate additional systems with the aim to manage data and users which form large bases. This integration of different systems is a challenge because access controls need to be maintained. In addition to all aforementioned, healthcare institutions are obliged to strictly adhere to the applicable regulations. Healthcare institutions must have strategy for secure access to health information system before they integrate blockchain/cloud computing with the aim to decentralize access. It is necessary to implement encryption, multi-factor authentication and programs for awareness and training.

Regular assessments of security practice and regular audits of system are absolutely necessary. These activities can clearly identify and reduce potential risks and threats to health information system. Secure access control is limited by technical infrastructure in hardware or software which can jeopardize system security and allow unauthorized access to medical data. Therefore, technical infrastructure must be regularly updated. Healthcare professionals can also compromise system security with inadequate use of medical data, with or without real intention. All this can lead to data breaches and other possible security issues with negative outcomes. Every weakness in secure access control must be recognized for true improvement of security and privacy. Monitoring and evaluation of security level is continuous process for identification of potential weakness of the system.

Implementation of comprehensive training and awareness programs for employees is also crucial because they emphasize awareness about potential issues and risks regarding to security and privacy of medical data. These trainings significantly reduce data breaches. Advanced multi-factor authentication additionally reinforces security level, minimizes the risk for unauthorized parties to access medical data and consequently minimizes the risk to data breaches (Arain et al., 2019; Mikuletič et al., 2024; Shojaei et al., 2024).

SECURE DATA SHARING

Secure data sharing in health information system refers to special aspect of security. It incorporates decentralization which reduces costs for healthcare institutions. There is also possibility to secure data sharing by centralization which is easier to secure and monitor. Secure data strengthens patients for management of their data whereby they fully control permissions for data sharing. Secure data sharing is complex process. Implementation of authentication and authorization is big challenge for large healthcare institutions which often use different standards and technologies which additionally complicate data sharing and leads to incomplete records. Prevention of data breaches is crucial because it leads to malicious use of medical data. It is possible to use firewalls and other security protocols and detection systems for invasion. Employees must pass through comprehensive training and awareness programs which emphasize the significance of security and privacy of sensitive medical data. Employees should be familiar with strategies and protocols which prevent risks related to data breaches. Data sharing has crucial role in the enhancement of patient care. Inadequate interoperability and lack of standardization are significant barriers for secure data sharing in health information system which leads to incomplete record. This issue manifests especially when different organizations provide care for one patient. Additionally, legal barriers often prevent data sharing between healthcare institutions, so patients are limited for benefits of this process. Inadequate cybersecurity and technical weakness jeopardize medical data, influencing their overall integrity availability and especially to their confidentiality.

Health information system needs to provide enough capacity regarding to large-scale data sharing and to integrate security features for protection of sensitive medical data. Improvements of interoperability involve adaptation of standard protocols for data sharing. Cybersecurity measured must be significantly reinforced along with continuous system security audits und updates. It is also important to overcome legal barriers which compromise efficient data sharing. Data sharing system should be designed based on practical needs. Implementation of data securitization ensures consistence through various systems and improves the level of quality of provided patient care (Shojaei et al., 2024).

It is not easy to achieve collaborative care of fully established operability. Significant challenge for patient is complex design of data consent policy and the application of tools related to e-health (health websites, mobile applications, different types of sensors, wearables) which often lack compliance with applicable regulations (Yigzaw et al., 2022).

Medical data reuse is related to research, quality of care, biosurveillance and health insurance issues. It is necessary to secure aggregated medical data from various healthcare providers. In the same time it is obligatory to preserve patients' privacy and to obtain consent from patient (Yigzaw et al., 2022).

SECURE DATA STORAGE

Secure data storage is significant aspect of security which ensures data security and privacy and reduces the risk of data breaches. Decentralization addresses security issues through smart contracts. Secured data storage preserves the confidentiality of medical data because only authorized parties are allowed to access, so data breaches is rather prevented. These secured data storages ensure trust between patient and employees in healthcare institutions which positively influence to treatment outcome and higher level of satisfaction with provided care. Secure data storage also ensures integrity, accuracy and relevance for decision-making. Patient medical data privacy and security depend on secured data storage. The advantages of this approach relates to increased trust of the patient, better compliance and cost-effectiveness. Challenges related to this issue encompass the implementation of stronger authentication and authorization which ensures that these data can be accessed exclusively by authorized parties. Security approach is multi-level and includes encryption, firewalls and invasion detection systems which prevent potential cyber threats and positively influences secure data storage.

It is necessary to have integrated, accurate and complete medical data about patient in order to provide adequate care and appropriate decision-making process enhancing overall quality of provided care for specific patient. Mechanisms for data recovery and backup reduce the risk of losing the data (Shojaei et al., 2024).

CONCLUSION

Digital transformation in healthcare industry refers to the usage of digital technologies for improvement of healthcare quality and patient treatment outcomes. High usage of digital technologies makes users vulnerable to cyber-attacks and threats to jeopardize integrity of medical data. Transdisciplinarity is an efficient approach to additional knowledge improvement. Health information system needs to fulfill organizational requirements and to protect patient medical data.

The role of health information system relates to storage retrieving, analysis, sharing and exchange of patients medical information. This system benefits patients and employees in healthcare institutions protecting the security and privacy of sensitive medical information, as its primary goal. Secure technologies must be applied for data sharing, data storage and access controls. It is of crucial importance to educate healthcare provider employees about topics related to patient data security and privacy. Key technologies in health information system are mobile health applications, IoT, blockchain and cloud computing. Future challenges and developments in this security field should integrate open electronic health records with available technologies in order to satisfy the needs of healthcare system with special focus to secured management of health information.

Modernization of technical infrastructure, comprehensive awareness and training programs predetermined for employees, adequate processes of authentication, continuous security audits and assessments contribute to improvement of security of health information system, reducing the unauthorized access and increase data protection.

REFERENCE LIST

AI-Issa, Y., Ottom, M.A. & Tamrawi, A. (2019). eHealth cloud security challenges: A Survey. *Journal of Healthcare Engineering*, 7516035.

Alzu'bi, A., Alomar, A., Alkhaza'leh, S., Abuarqoub, A. & Hammoudeh, M. (2024). A review of privacy and security of edge computing in smart healthcare systems: issues, challenges, and research directions. *Tsinghua Science and Technology*, 29(4): 1152−1180.

Arain, M.A., Tarraf, R. & Ahmad, A. (2019). Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. *Journal of Multidisciplinary Healthcare*, 12.

Arul, R., Al-Otaibi, Y.D., Alnumay, W.S., Tariq, U., Shoaib, U. & Piran, M.D.J. (2024). Multi-modal secure healthcare data dissemination framework using blockchain in IoMT. *Personal and Ubiquitous Computing*, 28, 3–15.

Bigini, G. & Lattanzi, E. (2022). Toward the interplanetary health layer for the Internet of Medical Things with distributed ledgers and storages. *IEEE Access,* 10: 82883-82895.

Bronsoler, A., Doyle, J. & Van Reenen, J. (2022). The impact of health information and communication technology on clinical quality, productivity, and workers. *Annual Review of Economics*, 14:23–46.

Czupryński, A., El Ghamari, M. & Zboina, J. (2021). Interdisciplinary and transdisciplinary security research. *European Research Studies Journal*, XXIV, 3B: 434-455.

van Drumpt, S., Timan, T., Talie, S., Veugen, T. & van de Burgwal, L. (2024). Digital transitions in healthcare: the need for transdisciplinary research to overcome barriers of privacy enhancing technologies uptake. *Health and Technology,* 14:709–723.

Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P.S., Swaminathan, A., Jahangir, M.M., Chowdhry, K., Lachhani, R., Idnani, N., Schumacher, M., Aberer, K., Stoller, S.D., Ryu, S. & Wang, F. (2020). ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. *Journal of Medical Internet Research*, 22(8):e13598.

Elhoseny, M., Thilakarathne, N.N., Alghamdi, M.I., Mahendran, R.K., Gardezi, A.A., Weerasinghe, H. & Welhenge, A. (2021). Security and privacy issues in medical Internet of Things: overview, countermeasures, challenges and future directions. *Sustainability*, 13(21), 11645.

Ferdousi, B. (2024). The importance of defining cybersecurity from a transdisciplinary approach. J*ournal of Systemics, Cybernetics and Informatics*, 22(1): 150-164.

Galea, S., Abdalla, S.M. & Sturchio, J.L. (2020). Social determinants of health, data science, and decision-making: Forging a transdisciplinary synthesis. *PLoS Medicine*, 17(6): e1003174.

Kelly, J.T., Campbell, K.L., Gong, E. & Scuffham, P. (2020). The Internet of Things: impact and implications for health care delivery. *Journal of Medical Internet Research*, 22(11):e20135.

Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M., Vahedi, F., Mehraeen, E. & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. *Journal of Medicine and Life*, 14(4), 448.

Mikuletič, S., Vrhovec, S., Skela-Savič, B. & Žvanut, B. (2024). Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. *Computers & Security*, 136, 103489.

Shojaei, P., Vlahu-Gjorgievska, E. & Chow, Y.-W. (2024). Security and privacy of technologies in health information systems: A systematic literature review. *Computers*, 13, 41.

Stoumpos, A.I., Kitsios, F. & Talias, M.A. (2023). Digital transformation in healthcare: technology acceptance and its applications. *International Journal of Environmental Research and Public Health*, 20, 3407.

Simplicio, M.A., Iwaya, L.H., Barros, B.M., Carvalho, T.C.M.B. & Näslund, M. (2015). SecourHealth: A delay-tolerant security framework for mobile health data collection. IEEE *Journal of Biomedical and Health Informatics*, 19(2): 761-772.

Saini, A., Zhu, Q., Singh, N., Xiang, Y, Gao, L. & Zhang, Y. (2021). A smart-contract-based access control framework for cloud smart healthcare system, *IEEE Internet of Things Journal*, 8(7): 5914-5925.

Sanka, A.I. & Cheung, R.C.C. (2021). A systematic review of blockchain scalability: Issues, solutions, analysis and future research. *Journal of Network and Computer Applicatons*, 195, 103232.

Shakil, K.A., Zareen, F.J., Alam, M. & Jabin, S. (2020). BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. *Journal of King Saud University - Computer and Information Sciences*, 32(1): 57-64.

Tong, Y., Sun, J., Chow, S.S.M. & Li, P. (2014). Cloud-assisted mobile-access of health data with privacy and auditability. IEEE *Journal of Biomedical and Health Informatics*, 18(2): 419-429.

Ullah, I., Amin, N.U., Khan, M.A., Khattak, H. & Kumari, S. (2021). An efficient and provable secure certificate-based combined signature, encryption and signcryption scheme for Internet of Things (IoT) in mobile health (M-Health) system. *Journal of Medical Systems*, 45(1): 4.

Yigzaw, K.Y., Olabarriaga, S.D., Michalas, A., Marco-Ruiz, L., Hillen, C., Verginadis, Y., Oliveira, M.T.D., Krefting, D., Penzel, T., Bowden, J., Bellika, J. G., & Chomutare, T. (2022). Health data security and privacy: Challenges and solutions for the future. In *Roadmap to Successful Digital Health Ecosystems: A Global Perspective,* 335-362, Elsevier.

Xie, Y., Zhang, K., Kou, H. & Mokarram, M.J. (2022). Private anomaly detection of student health conditions based on wearable sensors in mobile cloud computing. *Journal of Cloud Computing*, 11, 38.

Qiu, H., Qiu, M., Liu, M. & Memmi, G. (2020). Secure health data sharing for medical cyber-physical systems for the healthcare 4.0. *IEEE Journal of Biomedical and Health Informatics*, 24(9): 2499-2505.

***Milan Miljković*[1]**
***Hatidza Beriša*[2]**
***Marko Marjanović*[3]**

THE MULTIDISCIPLINARITY OF STRATEGIES TO DETER HYBRID THREATS

Abstract

The topic of hybrid threats, which has dominated the academic discussions among security scholars in the first decades of the 21st century, represents the most modern phase in the evolutionary development of conflict management, which includes military and non-military activities carried out by state and non-state actors. The aim of the research is to determine whether the current theory and practice of deterrence strategy is also relevant for deterring hybrid threats, or whether they require a more significant multidisciplinary character, bearing in mind that their conceptual model is based on four main pillars: the numerous actors and targets of hybrid threats, the multiple domains of implementation, the multidisciplinary nature of the tools for implementation, and the numerous phases of implementing hybrid threats. The author of the research begins with the hypothesis that a certain number of activities outlined in classical deterrence theory can also be applied in the strategy of deterring hybrid threats, but that they are not sufficient due to the specificity of these threats. The paper discusses the subject of research using the methods of comparative analysis of classical and contemporary deterrence theory and expert analyses of the characteristics of hybrid threats. It is concluded that for effectively countering hybrid threats and the success of these strategies, their greater multidisciplinary content is mandatory, which implies the application of knowledge from various scientific disciplines, such as military science, international relations, psychology, economics, information security, communication studies, and others.

Keywords: *Hybrid Threats, Deterrence Strategy, Multidisciplinarity of Domains and Actors.*

INTRODUCTION

Hybrid threats, as a relatively new concept in the fields of security studies and military science, have not been thoroughly explored in the literature. Moreover, there is

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

[2] National Defense School, University of Defense, Belgrade, Serbia, berisa.hatidza@gmail.com

[3] National Defense School, University of Defense, Belgrade, Serbia, foka1box@gmail.com

no globally unified and universally accepted definition of hybrid threats or hybrid warfare. One definition is provided by the international organization "Multinational Capability Development Campaign" in its study on countering hybrid warfare. The organization defines it as the synchronized use of various instruments of power directed (tailored, designed) towards specific, concrete vulnerabilities across the entire spectrum of social life to achieve a synergistic effect (MCDC, 2019). Hybrid threats are designed to exploit weaknesses in a state's political, military, economic, social, infrastructure, and information domains. An activity becomes a hybrid threat when an adversarial actor intentionally combines and synchronizes actions across various domains of social life, particularly targeting the systemic weaknesses of modern societies drawing from tactics employed by adversarial states, non-state actors, and networks that aim to undermine the legitimate state system, attempt to achieve control, and weaken their opponents. Other important characteristics of hybrid threats include: a) the use of multiple synchronized tools, primarily non-military tools to create both linear and non-linear effects, b) the creation of ambiguity in terms of covert and convincing denial and concealment of true intent, c) the exploitation of seams and cracks in the organization of modern society, as well as between different jurisdictions, d) demonstrating deliberate manipulation of thresholds regarding detection and response, and e) the inclusion of elements that distract attention, such as action at one location while the target is elsewhere (Giannopoulos et al., 2020: 15).

Although there are academic perspectives that consider hybrid threats to be a new phenomenon, they are, in fact, not a novelty in the realm of security threats. They are as old as conflict and warfare, but repackaged and reinforced by changes in the dynamics of the security environment, new tools, concepts, and technologies, which expand their range and effectiveness in achieving several strategic objectives, such as undermining public trust in the institutions of the attacked state, deepening unhealthy polarization at the national level, and gaining geopolitical influence and power through inflicting damage and influencing the decision-making capabilities of the opponent's political leaders. As a result, it is no surprise that today's hybrid threats present serious and acute dangers to modern states and are being seriously analyzed within security institutions across Europe.

In this context, the goal of the research is to determine whether the current theory and practice of deterrence strategy is relevant for deterring hybrid threats, or if a more significant multidisciplinary approach is required, considering that the conceptual model of these threats is developed around four main pillars: the numerous actors and objectives of hybrid threats, the variety of domains for their implementation, the multidisciplinary tools for their execution, and the multiple phases involved in carrying out hybrid threats. The author begins the research with the hypothesis that certain activities listed in classical deterrence theory can be applied in the strategy for deterring hybrid threats, but that these are insufficient due to the specific nature of these threats, which is why knowledge from multiple scientific disciplines is necessary.

THE MULTIDIMENSIONAL NATURE OF HYBRID THREATS

The focus of the hybrid concept lies in non-military actions, where the use of information technology is prominent, while, in addition to state actors, non-state entities also act as direct agents of hybrid operations. In this way, the objectives are achieved without armed conflict, or with small-scale armed interventions, resulting in minimal losses for the attacking side (Bilal, 2021).

Based on various interpretations, it can be concluded that this represents a specific type of conflict characterized by distinctive non-military and military activities, or the synchronization of unconventional and conventional actions carried out by non-state and state actors without limitations of time or space. Hybrid threats represent potential complex multidimensional dangers that jeopardize someone's security, arising from the simultaneous actors combining all available means to achieve common objectives (Mitrović et al., 2022: 27).

As previously mentioned, hybrid threat activities are conducted across multiple domains using a combination of tools. Each tool targets one or more domains, or interconnected areas, by exploiting vulnerabilities or existing opportunities. Therefore, it is important to identify areas of interest or critical functions that a state must ensure are resilient to hybrid threat activities, as they are strongly linked to national security and the state's ability to make decisions. The list of domains essentially represents an expanded list of instruments of national power, whose foundational principles originate from Western military science (U.S. Joint Chiefs of Staff, 2017).

In the following sections, each domain (critical infrastructure, cyber, political, military, economic, informational, etc.) is briefly described, highlighting which components of the domain may be the target of hybrid threat activities, as well as the connections between domains. Domains should not be examined in isolation, as the impact on one domain may trigger cascading effects in another. In the analytical framework, an action targeting one domain is further analyzed to enable the display of first- and second-order effects on other domains (Cullen, 2019).

The dimension of critical infrastructure, essential services and supply chains, regardless of the nature of the hostile actor (state or non-state), can be attractive targets for intimidation and pressure. Activities could aim to: (a) degrade the quality of the goods and services offered (e.g. reduce availability, reliability), (b) destroy key parts of the infrastructure and (c) increase the cost of their operation.

The cyber dimension plays an exceptional and very specific role in relation to hybrid threats, not only because anything significant that happens in the real world, including all political and military conflicts, will also unfold in cyberspace. For national security planners, this includes cybercrime, propaganda, espionage, influence operations, terrorism, and even war itself.

Economic policy tools such as sanctions, taxation, embargoes, trade agreements, asset freezes, sterilized interventions, subsidies, tariffs, government borrowing, and debt forgiveness are used in this context (Fabre, 2018; Norris, 2016). In light of the need to maintain denial and avoid provoking open military conflict, the exploitation of the economic domain would rarely have the same objectives as an open military campaign. The goal of hybrid threat actions in the economic domain is to comprehensively weaken the target state by undermining public trust in democracy and government. For example, economic measures or policies may be used to increase political pressure (Blackwill & Harris, 2016), or economic coercion may aim to modify the state's foreign policy stance or weaken the resilience of its economy, society, and security. The preparation phase of hybrid operations through the application of economic measures can last for decades.

A country's military capabilities represent the cornerstone of its existence and projection of power. Both in modern and ancient history, superpowers have combined economic and military power. Undermining a country's military and defense capabilities can be a very effective tool for increasing influence, exerting pressure, and, in certain cases, preparing the ground for future military operations. Threatening a nation's military defense capabilities triggers a reaction from the affected country, leading to an increase in defense costs and the depletion of resources. This is an implicit way of exerting economic pressure.

Actions through the cultural domain involve the use of "cultural governance" by an aggressor state against the attacked state, with the aim of supporting hybrid attacks. The scope of cultural governance can be internal, external, or both. Internally, cultural statehood implies "the use of cultural and civilizational themes in an effort to define the fundamental elements of national identity," while as a foreign policy strategy, it seeks "to promote culture as a means of projecting an attractive image abroad" (Wilson, 2016). In the case that the cultural domain is attacked, this indicates that a state is most likely behind such an attack, and it is coordinated and intended to support the activities of other hybrid threats.

The social domain is typically used to generate, deepen, or exploit sociocultural divisions, which will provoke the social upheaval necessary for the continuation or success of hybrid threat activities. Controversial issues such as unemployment, poverty, and education are always subjects of debate in societies and thus represent easy targets. The ultimate goal of actions in this domain will be to influence the way society functions in a way that strengthens divisions and internal discord, creating favorable conditions for hybrid threat activities.

An actor using hybrid threats can employ intelligence data in two main ways. Typically, they will use their own intelligence capabilities to support planned or ongoing hybrid threat activities, or they may attempt to influence the intelligence operations of the target state. In both cases, the actor seeks to undermine the target state’s ability to develop and maintain situational awareness, weaken decision-making capabilities at the political level, and diminish the capacity of public administration to implement policy.

Hybrid threat activities in the diplomacy domain are designed to create divisions at the national or international level, support all informational campaigns, and interfere in the decision-making process. The diplomacy domain has strong connections with the political domain. Although foreign policy is considered separate from domestic politics, these two are closely intertwined, primarily because negotiators in international politics must ratify their decisions by their domestic electorate. Therefore, diplomacy and domestic politics become a two-level game, requiring decision-makers to develop "sets" of solutions that can be defended both internationally and domestically (Putnam, 1988). In states, foreign policy supports domestic policy.

In the context of hybrid threats, the political domain includes actors, organizations, and institutions that exercise power or govern within a territory by applying various forms of political power and influence. Actors may attempt to exploit the political domain to influence the target state or establish favorable conditions for the execution of hybrid threat activities. Political power can be used either domestically or in the diplomatic arena. The tools of this domain target democratic processes, political organizations, and individuals. The political domain is strongly connected to diplomacy, largely due to the ability of foreign policy to have a significant impact on domestic policy. The relationship between the two is often described as a "two-level game" (Putnam, 1988).

The use of information as a weapon, and the informational domain as a space for conflict, has become a hallmark of hybrid threats and nonlinear strategies. The internet has become the leading and decisive substitute media. Tools of this domain seek to change political discourse, create or promote narratives, and manipulate public opinion and emotions. Furthermore, they can undermine freedom of thought and expression. The informational domain is strongly linked to the culture and social domains, as disinformation campaigns and other tools in this domain aim to influence the homogeneity of the culture and society of the target state.

HYBRID THREAT ACTORS

When theorists discuss actors and the ways in which they carry out their activities, they state that "hybrid wars can be waged by both states and various non-state actors. These activities can be carried out by separate units or even by the same unit, but they are generally operationally and tactically directed and coordinated within the main battle space to achieve synergistic effects in both the physical and psychological dimensions of the conflict" (Hofman, 2010: 444). The situation Hofman refers to here concerns wartime activities. However, in most of his works, the emphasis is on non-state actors. Ronald O'Rourke somewhat reflects Hofman’s views by listing three groups of actors: 1) revisionist powers, 2) rogue states, and 3) transnational organizations. He notes that, although different in nature and size, these rivals compete in political, economic, and military arenas, using technology and information to accelerate these competitions in order to alter the regional balance of power in their favor. He assesses that these are "essentially political struggles between those who favor repressive systems and those who favor free societies" (O’Rourke, 2018).

In accordance with the views of Hoffman and O'Rourke mentioned above, the focus in the context of hybrid threats today is mainly on state actors. Since states are still the most powerful challengers to other states or alliances, we generally think in terms of opposing states in the landscape of hybrid threats. However, this would be a potential oversight if non-state actors were not treated with equal seriousness. A quick review of the existing literature on hybrid threats reveals that the specificity of non-state actors in hybrid threat campaigns has not been the central focus of researchers and academics, despite the concept originating from non-state actions. Indeed, one of the first uses of the hybrid warfare concept was related to non-state actors. William Nemet studied the First Chechen War (1994-1996) and how the combination of modern political theory and technology with traditional ancient customs and ideologies in a decentralized, stateless society creating a unique capacity for warfare, which he termed "hybrid warfare" (Nemet, 2002).

When discussing states acting through non-state entities, this approach is referred to as "proxy warfare". When Frank Hoffman, inspired by Nemet, introduced the concept of hybrid warfare into the public debate in 2005 (Mattis & Hoffman, 2005), he associated it with Iran’s use of Hezbollah in its long-term low-intensity conflict with Israel. State actions through third parties or covert activities aimed at influencing and taking hostile measures against other states is certainly not a new phenomenon. An active non-state entity can take many different forms and may manifest itself through direct construction by a foreign state or a long-term ally formed through established relations and interdependencies, or shaped through short-term alliances to achieve common goals regarding local or specific problems, or through the manipulation of 'useful idiots' unaware they are advancing hybrid threat objectives.

Initially, it will be difficult to determine whether these activities are connected to covert state involvement. Knowing who the initiator of harmful events is will be of utmost importance in determining responses and ways to counter these threats in the future. For this reason, it is imperative that researchers not focus only on current events related to states in the domain of hybrid threats. It is also important to achieve a better understanding of the diversity of hybrid threats so that we can respond to the changing manifestations of future security challenges and limit their impact.

MULTIDISCIPLINARITY OF DETERRING HYBRID THREATS

The redefinition of strategy from a classical military science to a multidisciplinary science was dictated by political changes that gave rise to new theories of war, such as hybrid warfare, which increasingly incorporated non-military elements, such as the morale of the military and the people, political, economic, psychological, cultural, religious, and ideological contents, etc. Consequently, strategy had to encompass these elements as well, which inevitably led to a theoretical expansion of the concept of strategy.

It can be concluded that the understanding of the concept of strategy has significantly evolved within the scientific community, from its original military connotation to today's notion of strategy, which primarily implies civilian content. Thus, one can speak of the existence of, in addition to military strategy, state strategies, national strategies, political strategies, economic strategies, cultural strategies, demographic strategies, and so on. These terms are somewhat conditional, as they essentially refer to strategies aimed at social, political, economic, and cultural development. Within each of these specific sectoral strategies, strategies for the development of individual branches, fields, and the like can be discussed (Stojković, 2011: 46-58).

When considering deterrence strategies, it is important to begin by stating that deterrence aims to prevent the course of action by persuading a potential aggressor that the costs or consequences of their actions will outweigh the potential gain (Milkovski & Miljković, 2022).

There are three main pillars for achieving effective deterrence in practice: capability, credibility, and communication (Haffa, 2018). Capability refers to the ability or technical capacity to implement deterrence measures. Credibility is the willingness to carry out deterrence measures, while communication is a two-way understanding and perception that provides information about the cost-benefit calculations on both sides.

Experts today consider resilience to be the foundation of hybrid deterrence. Deterrence by denial is regularly advocated against hybrid threats, often in the form of resilience-building measures (Prior, 2018). Building resilience has itself become a strategy in an increasingly complex and unpredictable world. The recent rise of the practice and philosophy of cyber resilience in the civil sector may also influence thinking about resilience in national security. Just as in the case of cyber deterrence, retaliation against ambiguous or hard-to-detect hybrid threats may be less valuable than deterrence by denial (Morgan, 2012: 101).

Another advantage is that resilience measures focus on vulnerability and therefore do not rely on predicting the form of a hybrid attack. For all these reasons, resilience should form the foundation of any strategy for deterring hybrid threats. For example, a recent case study of the Dutch response to the downing of flight MH17 suggests that societal resilience – in this case, measured by the presence of trust, social capital, and credible narratives – strengthened deterrence (Doorn & Brinkel, 2020).

However, resilience is not a strategy in itself. In one sense, resilience is anti-strategic – it is passively inward-focused (on the ability to recover from shocks), rather than actively outward-focused on influencing others and shaping the environment. Resilience also has its limits. One is the difficulty in covering every possible attack vector. The literature emphasizes protecting the political and informational spheres of society, but these are porous domains that are less susceptible to government regulation than others, such as physical infrastructure (MCDC, 2019). As two Danish analysts have pointed out, “the facts on the ground currently make resilience a challenging if not Sisyphean task” (Sørensen & Nyemann, 2019). The desirability of large-scale resilience-building is also questionable. Paradoxically, overdoing resilience and government intervention within the liberal-democratic model may undermine the very fabric of society that one seeks to preserve, reinforcing a sense of threat and weakening “the cornerstones of Western democracy – state restraint, pluralism, free media, and economic openness” (Wigell, 2021: 49-67).

While deterrence by denial through resilience provides a solid foundation for deterring hybrid threats, changing the behavior of an adversary committed to hybrid aggression requires overcoming resilience to deter them through the credible threat of punishment. In practice, deterring hybrid threats necessitates finding the right balance between denial and punishment, tailored to the context and the actor in question (MCDC, 2019: 43).

It is also important to note the approach of restrictive deterrence, which suggests that when it comes to low-level hybrid threats, the focus should be on limiting rather than preventing such threats. Restrictive deterrence aims to minimize attributes such as effectiveness, frequency, or severity, but not to fully deter them. It is applicable to "persistent" but less severe hybrid threats. What counts as a "low-level" or "persistent" threat will depend on setting thresholds related to the type of threat (e.g., actor, domain, means) and the severity level at which the threat manifests (e.g., intensity, impact, and frequency). This type of hybrid threat – such as annoying disinformation or cyber disruptions – is not realistically deterrable in an absolute sense due to its ubiquity, low cost, denial potential, and limited impact (at least in the short term). Instead, it should be managed, tolerated, or mitigated. A good way to approach this discussion is to consider which hybrid threats can be tolerated, rather than which must be prevented (Rauta & Monaghan, 2021: 484). One parallel is crime prevention, where "not all crimes can be deterred, nor does every crime pose a significant threat to national security" (Wigell, 2021: 10).

Absolute deterrence seeks to prevent a particular action from happening entirely, rather than limiting or managing it. Given the military aspect of the dangers posed by hybrid threats – such as territorial loss, damage to critical infrastructure, erosion of a rules-based order, and even conventional or nuclear escalation – absolute deterrence is relevant at some level (Hersman, 2020: 90-109). However, the nature of hybrid threats – gradual, ambiguous and unconventional – makes it difficult to connect an immediate action that needs to be deterred with a specific outcome that must be avoided, or even with a specific actor that needs to be deterred. Restrictive deterrence, therefore, may be a more useful and reliable concept against most forms of hybrid aggression – at least all but the most obvious, severe, or totemic ones. The difficulty lies in agreeing on such thresholds. This is challenging enough among domestic policies, and potentially even more so in a multinational context. Nevertheless, this is precisely the challenge hybrid threats present – hence calls to align new collective thresholds, such as loss of life, e.g., via cyberattacks (Braw, 2022).

Due to all the aforementioned points, theorists emphasize the need to conceptualize a new form of deterrence against hybrid threats. While deterrence from military hybrid threats remains the primary goal (due to the potential costs of failure), the main focus is shifting towards deterring threats that are less lethal but more frequent. These are predominantly non-military hybrid threats that encompass a wide range of authorities and society, increasingly blurring the boundaries between international and domestic, collective and individual spheres. The complexity, diversity, and scope of the threats, actors, and targets – and thus the scope of deterrence actions – are unprecedented.

As a result of these new characteristics in the deterrence environment, the emphasis of deterrence strategy will shift from punishment to denial through resilience. The military and the government will rely less on relevant levers of power and means of deterrence, and more on the entire society, integrated into the fabric of everyday life.

In light of the above, deterrence encompasses two axes of strategies that can be employed against hybrid threat actors. The combination of these two axes provides a full conceptual range of strategy types for application in the context of hybrid threats. The framework of multidisciplinary deterrence strategies draws on and expands the research of King Mallory on various strategies in his 2018 analysis of multi-domain deterrence (Mallory, 2018).

The vertical axis consists of five general strategies: cooperation, persuasion, protection, coercion, and control. These five strategies differ in their use of incentives and disincentives – commonly referred to as the carrot and stick approach to influence the behavior of the other side, as explained below. Cooperation is the pursuit of mutually beneficial policies to maximize bilateral gains for both the source and the target through entanglement, reconciliation, and adaptation. Persuasion uses rewards to achieve cooperation with the opposing side, as an alternative to continuing confrontation. Protection aims to increase the source's ability to withstand or absorb hostile measures and usually results in win-lose scenarios. Two primary forms of protection are resilience and defense. Coercion, as opposed to cooperation and persuasion that focus on reward, involves persuading opponents through negative means. It forces the other actor to do something they do not want to do through deterrence and coercion. Control refers to the use of force to restrict the freedom of action of the target. Successful control typically leads to win-lose scenarios. Control strategies include prevention or preemption (Sweijs et al., 2021).

These five strategies can be used simultaneously or sequentially. In both cases, strategies should be applied carefully to correct each other's shortcomings and improve their potential. Some strategies, such as cooperation and protection, always reinforce each other's potential. Other strategies, such as control and persuasion, will undermine each other if used in tandem. All strategies have certain limitations and risks of failure, so no single element can serve as a unique means to ensure security (Mallory, 2018).

In addition to the vertical strategy options for (de)escalation, a horizontal axis of strategies can also be used. For this framework, the well-known DIME(L) categorization of state power instruments and measures is utilized, making a distinction between the diplomatic, informational, military, economic, and legal domains. Vertical measures escalate within the same domain. For example, if hostile measures revolve around cyber espionage, a vertically escalating response might involve acts of cyber sabotage. In contrast, horizontal escalation refers to expanding the scope of efforts beyond one DIME(L) domain to other domains. For example, diplomatic and economic sanctions can be used in response to military aggression, as the West did after Russia's annexation of Crimea. One level deeper, horizontal escalation can also occur within different military domains. Israel, for instance, used airstrikes on Hamas in the spring of 2019 as retaliation for a series of cyberattacks, employing kinetic countermeasures against cyber threats (Sweijs et al., 2021).

CONCLUSION

The aim of this paper is to present a comprehensive multidisciplinary array of strategies that can be employed in the deterrence of hybrid threats. Consequently, a range of strategies may be applied concurrently or sequentially to counteract hybrid threats. These strategies encompass cooperation, persuasion, protection, coercion, and control, and can be implemented across six distinct domains: diplomatic, informational, cyber, economic, military, and legal. Deterrence within each of these domains is operationalized through the application of both theoretical and practical insights drawn from a diverse array of academic disciplines and fields of study.

In relation to the aforementioned strategies, three key characteristics should be highlighted, which underscore their multidisciplinary nature. First, the strategies exhibit varying potential for escalation. Cooperation is the least escalatory strategy, as it aims to create mutually beneficial situations wherein all parties involved derive positive outcomes. Persuasion is somewhat more escalatory, as it entails subjecting the opponent to one's will while simultaneously offering incentives for cooperation. Protection represents a further step in escalation, as the opponent derives neither gain nor loss from its implementation. Coercion is even more escalatory, seeking to generate clear win-lose scenarios. Finally, control strategies are the most escalatory, as they aim to impose a decisive defeat on the adversary. This pattern highlights that the application of these strategies requires knowledge and insights from military sciences, as well as psychological and social sciences.

Second, the effectiveness of these strategies is contingent upon the specific characteristics of the domains in which they are applied. For instance, while diplomacy is as ancient as statecraft itself, modern communication technologies have revolutionized the speed and frequency of negotiations. Similarly, the contemporary informational environment exacerbates the asymmetry between attack and defense, as the attack surface of open societies is vast and increasingly vulnerable to both state and non-state aggressive actors. In a similar vein, the growing prominence of cyberspace as a strategic domain presents novel challenges to traditional deterrence, owing to its inherent ambiguity and the relatively low cost of launching attacks, juxtaposed with the high cost and often limited effectiveness of defensive measures. Meanwhile, the military instrument retains its unique position, as it is the only domain where direct application of force and harm is possible. In contrast, the economic domain continues to rise in importance, driven by the increasing interdependence of the public and private sectors. In comparison to other domains, the power of law is most heavily reliant on the perception and commitment of all parties involved. However, even in an antagonistic global context, law remains a relevant instrument, primarily because adherence to legal principles can offer moral leverage that may be strategically advantageous. Each domain, therefore, offers its own set of opportunities and limitations, necessitating careful consideration before selecting a particular strategy. As such, deterrence in each domain must be grounded in the specific body of knowledge relevant to that domain, including fields such as international relations, information security, communication studies, economics, and beyond.

The theoretical assumptions outlined above warrant further empirical testing, as while the underlying logic of the conceptual framework for deterrence may appear unequivocally clear in theory, strategic practice may challenge or undermine some of these theoretical presuppositions. To this end, simulation methodologies, particularly in the form of tabletop wargames, can be employed to elucidate how these strategies function within a controlled, competitive environment. The results derived from such exercises will help refine the framework and contribute to the development of more effective, domain-specific deterrence strategies in real-world scenarios. Ultimately, the successful validation of these strategies necessitates a thorough understanding of methodology, with particular emphasis on simulation techniques and wargaming practices.

REFERENCE LIST

Bilal, A. (2021). *Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote*. NATO Review, November 30.

Blackwill, R. D, & Harris, J. M. (2016). The Lost Art of Economic Statecraft. *Foreign Affairs* 95 (2): 99–110.

Braw, E. (2022). Biden's Gray-zone Gaffe Highlights a Real Dilemma. *Defense One*, January 20.

Cullen, P.J. Reichborn-Kjennerud, E. (2017). *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*.

Giannopoulos, G., Smith, H., Theocharidou, M. (2020). *The Landscape of Hybrid Threats: A conceptual model, European Commission,* Ispra, PUBSY No. 123305.

Haffa, R. (2018), "The Future of Conventional Deterrence: Strategies for Great Power Competition". *Strategic Studies Quarterly,* Volume 12, Issue 4, Winter 2018: 96-97.

Hersman, R. (2020), Wormhole Escalation in the New Nuclear Age, T*exas National Security Review*, Volume 3, Issue 3 (2020): 90-109.

Hoffman, Fr. (2010). Hybrid Threats: Neither Omnipotent Nor Unbeatable. *Orbis* 54 (3): 441–55.

Mallory, K. (2018). New Challenges in Cross-Domain Deterrence. Santa Monica: RAND Corporation, 2018).

Mattis, J. N. Hoffman, F. G. (2005). *Future Warfare: The Rise of Hybrid Wars,* November 18–19.

Milkovski, V. Miljković, M. (2022). Interakcija strategije prisile i odvraćanja – pouke iz agresije na Saveznu Republiku Jugoslaviju 1999. godine. *Politika nacionalne bezbednosti*. godina XIII, vol. 22, broj 1: 41–66.

Mitrović, M. Nebojša, N. (2022). *Hibridni rat*. Beograd: Medija centar „Odbrana".

Monaghan, S. Cullen, P. Wegge, N. (2019). MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare, January 2019.

Morgan, P. (2012). The State of Deterrence in International Politics Today. *Contemporary Security Policy*, Volume 33, Issue: 101.

Nemeth, W. J. (2002). *Future War and Chechnya: A Case for Hybrid Warfare*. Monterey: Naval Postgraduate School. U.S.

O'Rourke, R. (2018). A Shift in the International Security Environment: Potential Implications for Defense. Issues for US Congress. October 24, 2018.

Prior, T. (2018). *Resilience: The 'Fifth Wave' in the Evolution of Deterrence. Strategic Trends.* Center for Security Studies, ETH Zurich.

Putnam, R. D. (1988). Diplomacy and Domestic Politics: The Logic of Two-Level Games. *International Organization* 42 (3): 427–60.

Rauta, V., Monaghan, S. (2021). Global Britain in the grey zone: Between stagecraft and statecraft. *Contemporary Security Policy*, Routledge,Volume 42, Issue 4 (2021): 484.

Sørensen, H. Nyemann, D. B. (2018). Going Beyond Resilience - A revitalized approach to countering hybrid threats, *Hybrid CoE Strategic Analysis* 13, November 2018.

Stojkovic, B. (2011). Mesto strategije u društvenim naukama, *Vojno delo*, leto 2011, Beograd.

US Joint Chiefs of Staff. (2017). Joint Warfare of the Armed Forces of the United States - *Joint Publication 1*.

Van Doorn, C., Brinkel, T. (2020). Deterrence, Resilience, and the Shooting Down of Flight MH17. *Netherlands Annual Review of Military Studies*. 04 December 2020.

Wigell, Mikael. (2021). Democratic Deterrence: How to Dissuade Hybrid Interference. *The Washington Quarterly,* Volume 44, Issue 1 (2021): 49-67.

Wilson, Jeanne L. (2016). Cultural Statecraft in the Russian and Chinese Contexts: Domestic and International Implications. *Problems of Post-Communism* 63 (3): 135–45.

***Gordana Mišev*[1]**
***Marija Bajagič*[2]**
***Jelena Ignjatovič*[3]**

EDUCATION, DEVELOPMENT AND SECURITY – SCANDINAVIAN CASE STUDIES

Abstract

The links between education, development and security have not been sufficiently researched or conceptualized, although their correlation is undeniable. The fact is that states devastated by constant political tensions and armed conflicts cannot provide quality public services, including education, and therefore social and economic development, as a prerequisite for political and military power. Developed Western countries are characterized by political stability, democracy, economic development and peace. The subject of the paper is the analysis of reports that assess states according to the factors of political stability, democracy, quality of life and quality of education. The Scandinavian countries were singled out through the application of quantitative and qualitative methodologies. These countries are also known as welfare states, which foster the policy of the so-called Nordic peace. The aim of the paper is to explain the correlation between education, economic development and security and their mutual influence.

***Keywords**: Peace, Development, Education, Security, Scandinavian Countries.*

INTRODUCTION

The United Nations Development Policy and Analysis Sector uses the World Economic Situation and Prospects (WESP) dataset, which categorizes all countries in the world into one of three broad categories: developed, developed economies, and developing economies (UN/DESA, 2013). The tripartite division of the world in the 21st century refers not only to the degree of economic development, but also to the degree of regional and national security. The characteristics of developed countries are political stability, security, and peace, while post-socialist, post-colonial, and developing countries are characterized by political instability and conflict. However, underdeveloped countries and regions of protracted conflict, such as the Middle East and North Africa, are the greatest concern for the international community. Post-socialist and post-colonial

[1] Faculty of Diplomacy and Security, University Union-Nikola Tesla, Belgrade, Serbia, gmisev77@gmail.com

[2] Faculty of Agriculture, University of Bijeljina, Bosnia and Herzegovina, marijacvijanovic@yahoo.com

[3] Academy of Applied Studies Šabac, Serbia, jignjatovic985@gmail.com

countries, exhausted by economic recession and often accompanied by internal conflicts, lack the capacity to implement measures that would change both their political and economic systems. Additionally, they face challenges in transforming social awareness and social, cultural, and traditional values (Mišev, 2022). The positive effects of change are lacking. Transitions have dragged on for years, and human discontent has once again led to protests and conflicts (Serbia, Georgia, Ukraine, Somalia, Ethiopia). Even territories under the protectorate of Western powers – such as Afghanistan, Iraq, Bosnia and Herzegovina, Libya, and Kosovo – have failed to build stable democratic institutions, initiate economic development, and ensure security at all levels. A crisis state is a state of acute stress, where governing institutions face serious challenges and are potentially unable to manage conflicts and shocks (there is a risk of state collapse) (CSRC, 2006). Such a process could lead to the formation of new states, to war and unrest, or to the consolidation of the old regime. The opposite of a crisis state is a "resilient state", where institutions are generally capable of dealing with conflict, managing crises, and responding to disputes, whenever the state is between weakness and stability (CSRC, 2006). In this sense, we distinguish between weak (underdeveloped) and stable (developed) states, where the difference between stable (strong) and weak states does not indicate different phenomena or represent a systematic variation in this case; it is simply that most threats are more alarming for weak states (Buzan, Waewer, & de Wilde, 1998). Buzan (1991) states that the sectors of security (military, political, societal, economic, environmental) are interdependent and mutually conditioned. For example, an economic threat can affect the internal political stability of a state, and political instability can affect national security and open the door to external threats. If a state is weak, it is very susceptible to various types of security threats. These thematic frameworks are specifically applied to 4 areas of research: political legitimacy and institutional stability, democracy and the rule of law, economic development and education.

In response to the challenges posed by globalization in developing countries (Tošković, Filipović, 2017), a significant role has been assigned to education as part of the development of civilization and societal transformation. Education is part of the development of society as a whole (Pieczywok, 2018: 7). In the USA and other Western democracies, commitment to public education has gone hand in hand with growth and prosperity. Education is not static; it evolves with social changes. Educational systems reflect and shape the economic, social, cultural and political realities that operate at any time and in any place (Mazor, 2025). The new theory of economic growth emphasizes the fact that education has a strong impact on economic development. Numerous economists, including Harmon, Osterbeck, Gilmore, and Walker, argue that more educated countries not only develop faster but that educated citizens can contribute to and participate in local or regional political decisions in a meaningful way (Popescu and Diaconu, 2009). It is not surprising why Nordic countries, such as Norway, Finland, Sweden, and the Netherlands, with very high GDP per capita, have one of the most successful education systems (Popescu and Diaconu, 2009). As early as 1935, after the Great Depression, Lucien B. Keane attempted to link the shortcomings of the education sector to economic unreliability and insecurity. According to him, education is the main driving force for achieving interdependent goals (Veshapidze et al., 2021). In this sense, economic security can be considered a key indicator of the overall security of a state. Achieving economic security also facilitates other forms of security. In the context of modern security, education forms the strongest foundation for both individual and national economic security, which in turn becomes a stable and sustainable prerequisite for political, economic, social, and environmental stability (Veshapidze et al., 2021). Sustainable security can only be achieved when states and their institutions make education a priority. Learning drives change, change drives economic development, development enables political stability and ensures national security.

CORRELATION BETWEEN POLITICAL STABILITY, DEMOCRACY, DEVELOPMENT AND EDUCATION

To identify stable states, the following global reports were used: Fragile States Index (FSI, 2023); Democracy Index (DI, 2023) and Human Development Index (HDI, 2024). The Fragile States Index analyzes the weaknesses of states through four factors: 1. cohesion (security apparatus, factionalized elites and group grievances); 2. economic (economic decline, economic inequality and labor outflow); 3. political (state legitimacy, public services and human rights) and 4. social (demographic pressures, refugees and external intervention) (FSI, 2023). As democracy is a prerequisite not only for the rule of law, including basic human rights and freedoms, but also for electoral freedoms and the legitimacy of the Government, the Democratic Index was used, which includes five factors: 1. electoral process and pluralism, 2. civil liberties, 3. functioning of the Government, 4. political participation and 5. political culture (DI, 2023). The State Frailty Index reports on economic factors, including inequality, which is more of an economic policy issue, while the quality of life, or standard of living, indicates the level of economic, social, and human development. The Human Development Index analyzes 3 key dimensions of human development: 1. health, 2. education, and 3. standard of living (HDI, 2024). It was this report that turned the research in the direction of education analysis, so for the purposes of this work, the Report of the Marketing and Communications Company VPP in cooperation with the Wharton School of the University of Pennsylvania was used (USNEWS, 2024). Amartya Kumar Sen, an Indian economist who won the Nobel Prize in 1998 for his contribution to the economics of well-being, finds a direct link between education and human security, stating that education is a driving force in the fight for the emancipation of people from misery, insecurity and poverty (Khan, 2021). When it comes to quality of life, one of the key factors is the quality of education. This report was also used to assess the safest countries based on citizen perceptions (USNEWS, 2024).

The Fund for Peace's State Fragility Index provides practical tools and approaches for reducing conflict. It focuses on the link between human security and economic development. The Fund identifies the following countries as the least stable out of 179: Somalia, Yemen, South Sudan, Sudan, DR Congo, Syria, Afghanistan, Central African Republic (CAR), Chad, Haiti, and Ethiopia. These countries are ravaged by protracted political and armed conflicts. On the other hand, the most stable countries are (Table 1): Norway, Iceland, Finland, New Zealand, Switzerland, Denmark, Canada, Ireland, Luxembourg, and Sweden (FSI, 2023). What is evident is that stable states are democratic, developed countries, while the least stable states are characterized by a low level of democracy, i.e. all the listed weak states have an autocratic political system. Thus, according to the Democracy Index, out of 167 countries, Afghanistan is last at 167th place, the Central African Republic 164, Syria 163, Chad 161, DR Congo 160, Sudan 158, while there is no data for Syria, Yemen, and Ethiopia, which are war-torn countries. On the other hand, the countries with full democracy are: Norway, N. Zealand, Iceland, Sweden, Finland, Denmark, Ireland, Switzerland, the Netherlands, and Taiwan (DI, 2023). The Human Development Index out of 193 countries ranks Somalia at the lowest at 193rd place, J. Sudan 192, Central African Republic 191, Chad 189, Yemen 186, Afghanistan 182, DR Congo 180, Ethiopia 176, Sudan 170, Syria 157, etc. (HDI, 2024). During 2023, civil wars caused a huge number of civilian deaths, including Somalia, Ethiopia, Libya, Myanmar, Sudan, Syria and Yemen (DI, 2023). In Ukraine, Israel and Palestine, these processes are still ongoing, where the number of victims is constantly increasing.

The Human Development Index specifically analyzes average years of schooling. Consequences A nation's education can either improve a country's economic security or undermine economic stability (Muthanna et al., 2022). In Somalia, children attend school for an average of 1.9 years; in Chad 2.3; in Ethiopia 2.4; in Afghanistan 2.5; in Yemen 2.8; in the Central African Republic 4; in Haiti 5.6; in Syria and South Sudan 5.7; in the Democratic Republic of the Congo 7.2 years. The highest-ranked countries according to the Human Development Index (see Table 1) are Switzerland (13.9 years of schooling), Norway (13.1), Iceland (13.8), Hong Kong (12.3), Denmark (13), Sweden (12.7), Germany (14.3), Ireland (11.9), Singapore (11.9), and Australia (12.7) (HDI, 2024: 274-277). The feeling of being the safest is felt by the inhabitants of Switzerland, Norway, Sweden, Austria, Denmark, Canada, Finland, New Zealand and Australia (USNEWS, 2024). As seen, democratic countries with high political stability are also the safest, with a high Human Development Index. The common factor among these countries is a highly educated workforce (Table 2).

Table 1. *Ranking of countries according to political, democratic, human and security indices*

	Political stability index	**Democratic index**	**Human Development Index**	**The safest countries according to perception**
1	**Norway**	**Norway**	Switzerland	Switzerland
2	Iceland	N. Zealand	**Norway**	**Norway**
3	Finland	Iceland	Iceland	**Sweden**
4	N. Zealand	**Sweden**	Hong Kong	Austria
5	Switzerland	Finland	**Denmark**	**Denmark**
6	**Denmark**	**Denmark**	**Sweden**	Canada
7	Canada	Ireland	Germany	Finland
8	Ireland	Switzerland	Ireland	New Zealand
9	Luxembourg	The Netherlands	Singapore	Australia
10	**Sweden**	Taiwan	Australia	Belgium

Source: authors according to FSI, 2023; DI 2023; HDI, 2023; USNEWS, 2024.

Norway, Sweden and Denmark are in the top 10 ranked countries according to all analyzed factors, primarily when it comes to security. Switzerland is also in the top 10 countries according to all observed parameters, but the focus of the paper will be on the Scandinavian countries, due to their territorial proximity, specific international position and the policy of the so-called Nordic peace that characterizes them. Just as the Political Stability Index indicates not only political, but also economic, social and social parameters, the Democracy Index indicates the rule of law, freedom of choice and legitimacy of the government, the Human Development Index, in addition to health and quality of life, includes the most important segment of research, which is education. Quality education lays the strongest foundations for individual (micro-level) and national (macro-level) economic security, making it an indisputable prerequisite for a stable and sustainable political, economic and social environment (Ştefãnescu, 2022). In order to bring development, security and education closer together, it was necessary to extract the best ranked countries according to the quality, accessibility and level of education of the population. The ranking of countries according to the best education system (USNEWS, 2024), then accessibility, i.e. opportunities for free education (Mastersportal, 2025) and the assessment of the highly educated population (Eurostat, 2025), shows that the selected countries are also ranked among the top 10 countries in the world according to these factors (Table 2).

Table 2. *Ranking of countries by quality and accessibility of education*

The best education system	Free education	Percentage (%) of highly educated		
		25-34 years old	55-74 years old	25-74 years old
Denmark	Germany	35,4	28,1	32,4
Sweden	**Norway**	**52**	**35,1**	**46**
UK	Finland	43,9	35,4	40,5
Finland	**Sweden**	**53,6**	**35,1**	**46,9**
Germany	**Denmark**	**46,9**	**30,3**	**40,5**
Canada	Iceland	46,5	33,1	42,2
Norway	Austria	40,4	24,8	34,5
Japan	Greece	36,7	24	31,7
Switzerland	Malta	36,9	12,1	29,3
Australia	Cyprus	55,5	31	47,5

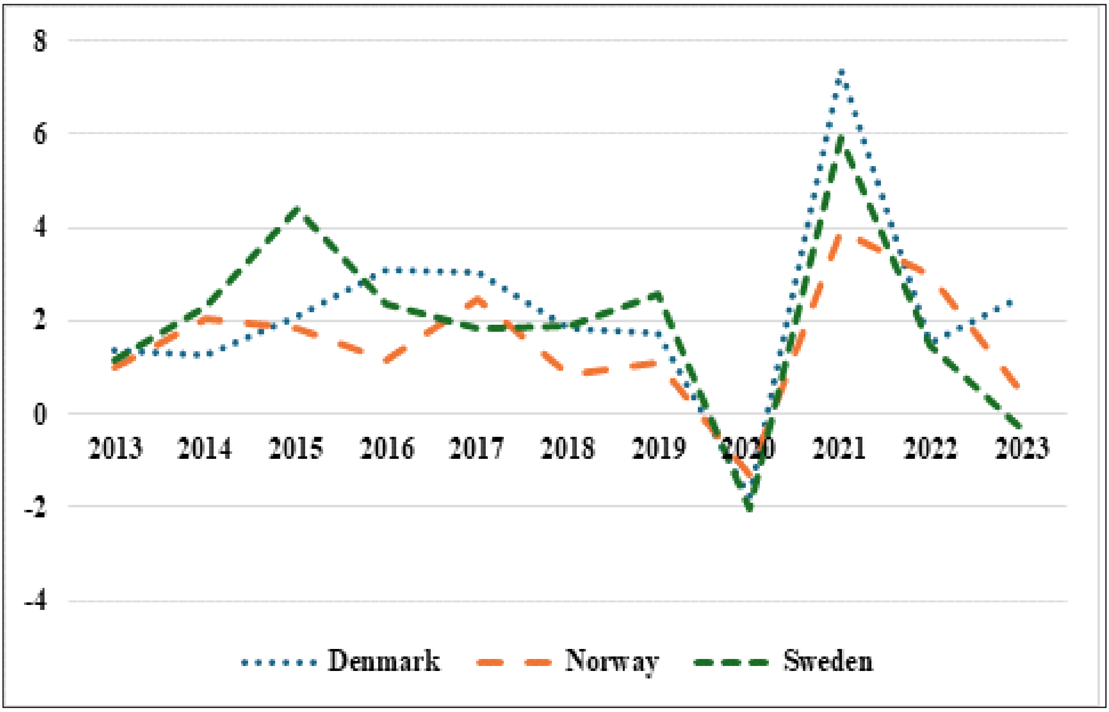
Source: authors according to USNEWS, 2024, Mastersportal, 2025; Eurostat, 2025.

The Scandinavian countries have a higher percentage of highly educated people than the EU average (32.6%). Denmark has 40.5%, Sweden and Norway around 46% of graduates with tertiary education. The data is particularly impressive for young people, as one in every two young people in these countries has a higher education. This shows that these countries have recognized the importance of education for overall development, stability and security, which is why there is a clear trend of growth in the number of highly educated people.

THE SCANDINAVIAN WELFARE COUNTRIES

The EFA 2013/4 (Education For All) Monitoring Report shows that “a one-year increase in the average education of a country’s population increases annual GDP growth per capita from 2% to 2.5%” (UNESCO, 2014: 151). A study conducted by Moretti in 1998 in the USA showed that in the 1980s, each additional year of education led to an average increase in income of 5.8%; in the 1990s, this coefficient almost doubled, reaching 10.9% (Popescu and Diaconu, 2009). Economic security is imperative for the formation of a stronger defense capability of a country. The study of economic security should be based on how a state uses economic mechanisms to maintain its territorial integrity, to what extent it satisfies the needs of its citizens, how it maintains political and cultural independence, and how it manages to avoid foreign military aggression (Dimitrijević, 2024). The Nordic countries (Norway, Iceland, Sweden, Finland and Denmark) continue to dominate the Democracy Index rankings, occupying five of the top six places. Norway is still the best-ranked country in the Democracy Index, thanks to high scores in all five categories of the index, especially electoral process and pluralism, political culture and political participation (DI, 2023: 15). Economic issues such as competition for resources are at the root of many contemporary conflicts, but they are not the only causes. Whether economic conflicts at the national or international level will lead to violent conflict or war is a matter of political choice (DI, 2023: 15). Therefore, the State Stability Index takes into account social and political factors in addition to the economic factor. In this sense, there is a clear correlation between all these factors and their conditioning, which create the so-called identity politics. welfare state, as well as their Nordic peace policies, based on the postulates of development, peace and stability. This is supported by economic growth, which in the period 2013-2023 totaled 2%. Although the economic decline was recorded during the pandemic period in 2020 (Denmark -1.7%, Sweden -2%, Norway -1.2%), a strong recovery followed the following year, when it reached a growth of 5.7% (Denmark 7.9%, Sweden 5.9%, Norway 5.9%). However, the onset of the energy crisis and the war in Ukraine led to a slowdown in growth, with Sweden entering a recession (-0.3%) (Graph. 1).

Graph 1: *Economic growth (%) in selected countries of Scandinavia*



Source: World Bank, 2025.

Norway

The Norwegian economy is characterized by economic growth, low unemployment and inflation, and low public debt (Table 3), while the financial sector is open and free (EFI, 2024). In the observed period 2013-2023, average economic growth was 1.5%, inflation was 4%, while unemployment was only 3.9%. Given that the Scandinavian countries have the highest public spending on education, in Norway it is 6.6% of GNI (Table 3) (World Bank, 2025). Public debt is on average 37.5% (Trading Economics, 2025).

Table 3. *Macroeconomic aggregates in Norway*

NORWAY	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
GDP growth (%)	1,0	2,0	1,9	1,2	2,5	0,8	1,1	-1,3	3,9	3,0	0,5
Unemployment (%)	3,4	3,5	4,3	4,7	4,2	3,8	3,7	4,4	4,4	3,2	3,6
Inflation (%)	2,6	0,3	-2,8	-1,6	4,1	6,7	-0,5	-2,5	20,2	28,2	-10,6
Central government debt (%GDP)	30,7	28,4	33,1	36,9	37,5	38,8	39,8	45,1	41,3	36,5	44,2
Education expenditure (%GNI)	6,6	6,7	6,4	6,7	6,6	6,4	6,7	6,7	6,7		

Source: World Bank, 2025; Trading Economics, 2025.

The successful education system is based on 20 public and three private university colleges. More than 90% of students attend public higher education institutions, and about 46% of Norwegians have a college or university degree. Norway fosters the Scandinavian social model with universal health care, subsidized higher education, and a broad social security system (Weebly, 2025). Education is key to sustaining high employment and fostering a productive, innovative workforce. The Norwegian school system is inclusive and free. There is a common national curriculum for primary and secondary education, but within this framework, municipal and county governments, schools, and teachers can influence the implementation of education and training (Eurydice, 2025). Political stability is contributed by an independent judiciary, protection of property, and especially the fight against corruption, in which Norway is among the leaders in the world. The labor outflow is low, primarily due to the developed economy and stable market. According to the Human Development Index, Norway is in second place, which indicates that in addition to the education system, the health system also functions excellently, which particularly contributes to the quality of life. Electoral pluralism and the legitimacy of the government speak of a developed democracy, which is stable thanks to the quality and accessibility of education.

Sweden

The Swedish economy is characterized by low unemployment, low inflation, and public debt and economic growth (EFI, 2024). In the observed period 2013-2023, the average economic growth was 2%, inflation was 2.8%, while unemployment was 7.5%, while the highest public spending on education was 7.1% of GNI (Table 4) (World Bank, 2025). Public debt is on average 42.5%, which is one of the highest debts in the three observed countries (Trading Economics, 2025).

Table 4. *Macroeconomic aggregates in Sweden*

SWEDEN	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
GDP growth (%)	1,1	2,3	4,4	2,3	1,8	1,9	2,5	-2,0	5,9	1,5	-0,3
Unemployment (%)	8,1	8,0	7,4	7,0	6,7	6,4	6,8	8,3	8,7	7,4	7,6
Inflation (%)	1,0	1,8	2,3	1,7	2,2	2,6	2,4	1,8	2,7	5,8	6,1
Central government debt (%GDP)	45,3	49,2	47,7	46,3	44,3	42,5	38,7	44,1	40,6	36,9	31,5
Education expenditure (%GNI)	7,1	7,0	7,0	7,2	7,1	7,1	7,1	7,1	7,1		

Source: World Bank, 2025; Trading Economics, 2025.

Sweden is often cited as a paradigmatic example of social democracy. It seems to have achieved, along with other Scandinavian countries, an excellent combination of social equality and economic efficiency (Stephens, 2001). Sweden was a poor country in the first half of the 19th century, when it began to allocate significant resources to education. Already in the second half of the 19th century, it had one of the highest growth rates in Europe (Šuković, 2013: 38). Today, Sweden has stable and long-term growth and is one of the so-called welfare states to which all Scandinavian countries belong. Sweden has free education and is the country with the highest public expenditure on education in relation to GDP in the EU, resulting in over 46% of people with higher education. It has a decentralized education system, governed by centrally defined learning objectives and outcomes. The government has overall responsibility and sets the framework for education at all levels (Eurydice, 2025). When it comes to political stability, Sweden has a legitimate government, an efficient public service, but under the impact of the migrant crisis, the rule of law is somewhat lower than in other analyzed countries, but certainly at a high level. It is characterized by a low outflow of labor, which shows a developed market and economic stability. Political stability is also built from economic stability, and democracy ensures the rule of law and free elections.

Denmark

The Danish economy is characterized by constant economic growth, low unemployment, low inflation (%), and low public debt (EFI, 2024). In the observed period 2013-2023, the average economic growth was 2.2%, inflation was 1.5%, while unemployment was 5.7%. Public spending on education is 6.7% of GNI (Table 5) (World Bank, 2025). Public debt is the lowest of the observed countries and is 36.6% (Trading Economics, 2025).

Table 5. *Macroeconomic aggregates in Denmark*

DENMARK	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
GDP growth (%)	1,4	1,3	2,1	3,1	3,1	1,9	1,7	-1,8	7,4	1,5	2,5
Unemployment (%)	7,4	6,9	6,3	6,0	5,8	5,1	5,0	5,6	5,0	4,4	5,1
Inflation (%)	0,8	1,0	0,4	0,4	1,1	0,6	1,0	2,8	2,8	9,1	-3,8
Central government debt (%GDP)	40,0	44,3	39,8	37,2	35,9	34,0	33,7	42,3	36,0	29,8	29,3
Education expenditure (%GNI)	7,7	6,9	6,8	6,7	7,2	6,2	6,2	6,2	6,2		

Source: World Bank, 2025; Trading Economics, 2025.

The rule of law is highly respected in Denmark, and an independent and corruption-free legal system provides strong protection of human and property rights. In Denmark, as in the other countries analyzed, almost half of the population has a higher education. Equal and free access to education for all: the Danish education system aims to ensure that all people acquire knowledge and competences that qualify them for active participation in society and contribute to its further development. Education is open to all and is generally free of charge. Institutions ensure that educational programs are relevant to society and oriented to meeting the needs of the labor market. There is a tradition of participation in education throughout all stages of life, i.e. the principle of lifelong learning (Eurydice, 2025). According to the Political Stability Index, Denmark has a developed rule of law and a high degree of legitimacy of the government, as well as an efficient public service, low labor outflow (FSI, 2023). Like all Western European countries, Denmark is facing an influx of migrants, but this has not yet affected political stability or security, primarily due to its developed democracy and human rights. There is a clear correlation between education, political stability, and economic development.

The Nordic countries have long been a region of peace, with the ability to peacefully resolve conflicts among themselves, which also actively promotes peace on a global level. The Nordic countries have built their political identity through the development of the so-called Nordic peace policy, despite being members of the military-political international organization of the North Atlantic Treaty Organization. This is best illustrated by the problem of the Åland Islands, which are claimed by both Sweden and Finland. The Åland Islands are a Finnish archipelago located in the Baltic Sea, 40 kilometers from Sweden and 95 kilometers from Finland. The Åland Islands have about 25,000 inhabitants, of whom 95% are Swedes and 4.5% are Finns. The League of Nations granted the Åland Islands autonomous status in 1921, and this dispute is often cited as an example of good practice for resolving the status of secessionist territories in Moldova, Ukraine, Georgia, Serbia, Azerbaijan, Somalia, etc. Social cohesion, minimal polarization of society, economic development, and above all trust in the Government and the rule of law contributed to the constructive resolution of the dispute over the Åland Islands.

Achieving social security and social peace depends on the regulatory quality that ensures the rule of law, including human rights and freedoms and the effective fight against crime and corruption. Although social and political stability are important factors, without economic development, there is no overall development of society. Along with the discovery of the key role of education in the overall multitude of development processes and in the expansion of the economy as a whole, the question arose very early on whether there was a place for the introduction of a new concept, namely educational capital (Madžar, 2013: 28). It is clear that the level of education correlates with the level of economic development and political stability. Weak or collapsed states such as Afghanistan, Syria, Somalia, Chad, Yemen, Ethiopia educate children for several years, which is not enough to acquire even elementary knowledge. In times of peace, these countries do not invest in education, but the international community focuses on democracy and the conduct of elections, as prerequisites for political stability and economic development. However, an uneducated population cannot contribute to democratic or constructive changes in a country. This is best demonstrated by Sweden, which, from an underdeveloped state in the 19th century, is now part of the developed, collective West. This analysis raises numerous questions regarding developing countries (Grujić, Ignjatović, 2024; Filipović, Ignjatović, 2021), that is, countries of hybrid democracy and political instability, which include almost all former socialist countries. These countries have undergone and are undergoing turbulent political changes and conflicts, including Serbia, Georgia, Ukraine, Moldova, Azerbaijan, Tajikistan, Uzbekistan, etc., and in early 2025, numerous political protests in Eastern Europe, including EU member states, raised the issue of economic development and sustainable progress of these countries.

CONCLUSION

Political stability, characterized by decentralization, good governance, trust in government, democratic political culture and, above all, the availability and level of education, have ensured stable economic development (low public debt, unemployment and inflation, stable GDP growth) and regional stability as key factors in the development and security of the analyzed Scandinavian countries (Denmark, Sweden, Norway).

Achieving social security and social peace depends on regulatory quality that ensures the rule of law, including human rights and freedoms, and an effective fight against crime and corruption. Although social and political stability are important factors, without economic development, there is no overall development of society, as the aforementioned Scandinavian countries have shown.

REFERENCE LIST

Buzan, B., Waewer, O. & de Wilde, J. (1998). *Security: a New Framework for Analysis*. Colorado: Boulder: Lynne Rienner.

Crisis States Research Centre (May 2006). *War, state collapse and reconstruction: Phase 2 of the Crisis States Programme*. Development studies institute - DESTIN, London

Democracy index. (2023). *Age of conflict*. The Economist Intelligence Unit: https://www.eiu.com/n/campaigns/democracy-index-2023/

Dimitrijević, D. (2024). Unapređenje evropske ekonomske bezbednosti: uvod u pet novih inicijativa. *Evropsko zakonodavstvo*, 23, 77-92.

EFI. (2024). *Index of Economic Freedom*. The Heritage Foundation: https://www.heritage.org/index/pages/all-country-scores

Ejdus, F. (2012). *Međunarodna bezbednost: teorije, sektori i nivoi*. Beograd: Službeni glasnik i Beogradski centar za bezbednosnu politiku.

Euronews (2025). Which countries are home to the most educated people in Europe? https://www.euronews.com/next/2024/08/17/which-countries-are-home-to-the-most-educated-people-in-europe

Eurostat (2025). Educational attainment statistics. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Educational_attainment_statistics

Eurydice (2025). National Education Systems. https://eurydice.eacea.ec. europa.eu/national-education-systems

Filipovic, S., Ignjatovic, J. (2021). International relations through the prism of the new technological division of power. *Međunarodni problemi*, Vol. LXXIII - Br. 4: 637-666. DOI: https://doi.org/10.2298/MEDJP2104637F

Filipović, S., Ignjatović, J. (2022). Ekonomski razvoj Zapadnog Balkana: šanse i ograničenja za zelenu tranziciju, *Megatrend Revija,* Vol.19 (3), pp. 167-182. DOI: 10.5937/MegRev2203167S

Fragile States Index (2023). *Annual Report*. https://fragilestatesindex.org/analytics/fsi-heat-map/

Grujić, D., Ignjatović, J. (2024). *Finansijski menadžment*. Šabac: Akademija strukovnih studija. http://www.vpssa.edu.rs/?page_id=19684

Human Development Report (2024). *Breaking the gridlock Reimagining cooperation in a polarized world*. https://hdr.undp.org/system/files/documents/global-report-document/hdr2023-24reporten.pdf

Khan, Z. (2021). *Relationship between Education and Human Security. The Human Security*. https://thehumansecurity.org/relationship-between-education-and-human-security/

Madžar, Lj. (2013). *Obrazovni sistem na tranzicionoj vetrometini − bespuća i mrtvouzice aktuelnih razvojnih alternativa. Obrazovanje i razvoj.* Institut drštvenih nauka i Centar za ekonomska istraživanja. http://www.idn.org.rs/biblioteka/Obrazovanje_i_razvoj.pdf

Masters study portal (2025). Free Universities in Europe in 2025. https://www.mastersportal.com/articles/3200/free-universities-in-europe.html

Mazor, K. (2025). Education for Our Times. The human journey. https://humanjourney.us/health/education-for-a-changing-world/education-in-the-modern-world-solving-for-the-future/?gad_source=1

Mišev, G. Z. (2022). *Faktori uspešnog razvoja država i njihove implikacije na bezbednost*, Doctoral dissertation, University of Belgrade, Serbia.

Muthanna, A., Almahfali, M., & Haider, A. (2022). The interaction of war impacts on education: Experiences of school teachers and leaders. *Education Sciences*, 12(10), 719.

Pieczywok, A. (2018). Security education in dangerous times. *Security and Defence Quarterly* 2018; 21(4) pp. 7-22

Popescu, C.C and Diaconu, L. (2009). T*he relationship between the level of education and the development state of a country*. ANALELE ştiinłifice ALE universitălii „Alexandru Ioan Cuza" Din Iaşi Tomul LVI ŞtiinŃe Economice, pp. 475-480

Scientia moralitas-*International Journal of Multidisciplinary Research*, 7(2), 106-121.

Ștefănescu, A. A. (2022). *Education in the Current Social, Economic and Security Environment*.

Tošković J., Filipović S. (2017), *Neoliberalni koncept privrede u zemljama Zapadnog Balkana*, Ekonomski Institut, Beograd. https://www.researchgate.net/publication/331565179_Neoliberalni_koncept_privrede_u_zemljama_Zapadnog_Balkana

Trading Economics. (2025). *Data*. https://tradingeconomics.com/norway/full-year-gdp-growth

U.S. News (2024). Most Well-Developed Public Education Systems. https://www.usnews.com/news/best-countries/rankings/well-developed-public-education-system

UNESCO (2014). *UNESCO education strategy 2014-2021*. UNESCO Digital Library : https://unesdoc.unesco.org/ark:/48223/pf0000231288

Veshapidze, S, Chiabrishvili, K, Zubiashvili, T. And Zoidze, G. (2021). On the relationship between education and economic security. *Ecoforum,* Volume 10, Issue 3(26). DOI:10.5281/zenodo.5806515

Weebly (2025). Norway. Weebly: https://norway-norveska.weebly.com/index.html

World bank. (2025). Data. https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?end=2022&start=1971

***Mina Zirojević*[1]**
***Darko M. Marković*[2]**

DARK NET, SOCIAL MEDIA AND EXTREMISM

Abstract

The recent IS attack in Jakarta highlights the increasing use of the dark web to conceal and protect terrorist communications. Radicalization via Internet networks, the spread of false and half-truths, and the recruitment of new members into terrorist organizations via the Internet have long been well documented. In June 2015, Beatrice Burton wrote about IS's superior messaging and engagement capabilities, which should direct us to achieve at least equal effectiveness in countering such activities. There is ample evidence that one of the reasons for the lack of success in the fight against radical extremism is the overanalysis of narratives. Responses to these direct narratives are often too academic and research-oriented, failing to reach the target groups. Most extremist movements convey a relatively simple message – one that is easy to understand and easy to accept. An effective counter-narrative should consist exclusively of photos, videos and 140 characters. No more, no less. In this paper, we answer the question of what an effective response should entail and what the success of its implementation depends on, despite potential challenges and obstacles.

Keywords*: Terrorism, Dark Web, Media, Narrative.*

INTRODUCTION

The digital world has changed the way we live, connect and interact. While once the fight against extremism meant following physical clues – meetings in secret rooms or letters passed through intermediaries – today the fight has moved to the invisible paths of the Dark Net and noisy social media platforms. It didn't take long for extremists to realize the power of these tools: from encrypted messages to viral videos recruiting young people from their bedrooms. Although it might seem at first glance, this is not just a technological change, but a new kind of struggle for simple messages to attract people's attention and loyalty. On the other hand, security forces and institutions often flounder, stuck in complex analyzes and responses that do not reach those for whom they are intended. This disparity between extremist skill and institutional inertia raises the question: how to restore balance in this struggle?

[1] Institute of Comparative Law, Belgrade, Serbia, mina.zirojevic@gmail.com

[2] Faculty of Law for Commerce and Judiciary in Novi Sad, University of Business Academy in Novi Sad, Serbia, darko.bg.ns@gmail.com

The aim of this research is to show why conventional responses to extremism fail and to offer a practical solution – a counter-narrative that can compete with extremist messages on their turf. It is not enough to understand how the Dark Net and social media work as weapons in the hands of terrorists; it is necessary to discover what we can do to surpass them. The paper starts from the assumption that the strength of extremists lies in the simplicity and emotions with which they win over the audience, while the official answers lose their impact due to excessive complexity and lack of human touch. The idea is not to create another complex plan that will end up in a drawer, but to offer something that can be implemented immediately - messages that fit into 140 characters, accompanied by images and videos that speak the language of communities. Therefore, the goal of this work is to show how powerful the understanding of people and their needs is as an approach in the effort to stop extremism.

The methodological process that led to these conclusions relies on a combination of analysis of existing examples and practical thinking about what works in the real world. First, it studied how extremists use the Dark Net and social media, looking at specific cases such as the Jakarta attack or Facebook recruitment. It then discusses why current responses – from academic studies to institutional campaigns – are not delivering, focusing on their weaknesses such as over-theorizing and neglecting the local context. Through this analysis, recurring patterns have been observed: extremists win because they are fast and close to the people, while institutions fall behind because they are slow and distant. Based on this, a counter-narrative built on simplicity and emotion is proposed and tested through examples of messages and visuals that could work. The work does not rely on complex statistics or models, but on the logic of everyday life – what would make someone choose a community instead of hatred that provides them with a sense of belonging, authenticity and an opportunity to express themselves through some activity. Finally, it discusses how this approach could be implemented and what obstacles stand in the way, giving a practical view of how to move from idea to action.

This paper is not just another theoretical discussion – it is a call to return the fight against extremism to where it is really fought: in the digital space where messages are born and spread. While extremists use the web as a megaphone for their ideas, we must learn to use it as a bridge to the public. If we can understand what drives them and give them something better to believe in, we can turn the tide of this fight. Everything starts with a simple step - speaking in a language that is heard and understood.

DARK NET AND SOCIAL MEDIA AS TOOLS OF EXTREMISM

Connectivity and the wider digital realm play a central role in shaping modern society. During the 21st century, the digitalization process brought, initially, many good things, such as the expansion of economic opportunities and the exchange of cultural goods, the connection of different cultures, and improved access to information and services for individuals around the world who would otherwise lack such opportunities. According to the International Telecommunication Union (ITU), in 2023, 67 percent of the world's population – or 5.4 billion people – had access to cyberspace (International Telecommunication Union [ITU], 2023). Today, that number is much higher. With the growth of the number of participants online, there is more and more misuse of it, so now all the criminal activities that we have in real life, we have online in an even worse form. This development has allowed extremists to use the Dark Net and social media as key tools for coordination, propaganda and radicalization (Weimann, 2016).

Increased concern about illegal activity on the dark web has been fueled by the emergence of a wider "criminal underworld" – online communities to coordinate illegal activity. The inclusion of the dark web is natural for this underground, as is its expansion into the wider ecosystem of the Internet, including increasingly encrypted communication platforms. The terms Deep Web, Deep Net, Invisible Net or Dark Web refer to the content of the deep part of the Internet that is not indexed by standard search engines. The deepest layers of the deep web, known as the dark web, contain content that is deliberately hidden, including illegal and anti-social information, such as terrorist communications (Chen et al., 2008). For example, Al Qaeda used encrypted messages left in the "drafts" folders of webmail services to avoid intelligence surveillance, while "Silk Road" coordinated illegal activities, earning over $1.2 billion in bitcoins before the arrest of founder Ross Ulbricht in 2013 (Zirojević Fatić, 2011).

Some phenomena are known or more advanced in the cyber world, for example the phenomenon known as "crime-as-a-service" - a business model in which criminals offer products or services to potential customers in exchange for a non-monetary fee. This model, also called "cyber-crime-as-a-service", allows individuals with varying degrees of technical expertise to engage in the criminal world alone or within a group structured as legitimate companies that employ teams of programmers, engineers and technical support representatives. Although this model is widespread in cybercrime, extremists adapt it for coordination and financing, facilitating cooperation among terrorists around the world and expanding the geographic scope of their activities (Zirojević Fatić, 2011).

The recent IS attack in Jakarta, Indonesia, shows the increasing use of the darknet to conceal and protect terrorist communications (Weimann, 2016). IS used encrypted platforms to plan and spread propaganda, while social media served to recruit and amplify messages. According to the "theater of terror" theory, such attacks are carefully designed to attract global attention, using simple, dramatic narratives (Jenkins, 1975, as cited in Zirojević Fatić, 2011). Hezbollah, for example, uses websites to publish "martyr" statistics and psychological pressure on Israelis, while Hamas recruits through Facebook and uses Google Earth to plan attacks, as seen in Mumbai in 2008 (Zirojevic Fatić, 2011).

If we go back to the beginnings of the Internet, we will see that its use was reduced to sending false truths and half-truths, as well as mutual communications between members of terrorist organizations. Of course, it is also related to the level of technological development and the possibility of content creation. Later, especially during the corona virus pandemic, the need to recruit new members through the network developed (Wimmer, 2016). However, the development of technology brought competent institutions to the door of criminals, and they fled to the edges of the Internet, that is, to the part that we colloquially call the "dark network" or darknet. Today, on the dark side of the Internet world, radicalization via the Internet, sending false and half-truths, recruiting new members of terrorist organizations, hiding and collecting money via the Internet, which has long been well documented (Weimann, 2016). Research confirms the rise of these activities on the Dark Web (Chen et al., 2008).

Security forces are still struggling to adequately respond to this threat. The main reason for the lack of success in the fight against radical extremism is the excessive analysis of the narrative, that is, the complexity of the answers. Terrorists spread propaganda and attract new supporters with simple language, facts and images, and the responses to this simple narrative are generally overly scientific, investigative and do not reach the target groups (Berton, 2015, as cited in Weimann, 2016). Most extremist movements carry a relatively simple message – a message that is easy to understand and adopt. An effective counternarrative should consist of only photos, videos and no more than 140 characters, opposing extremist propaganda on the same ground (Malik, 2018).

PROBLEMS WITH CONVENTIONAL RESPONSES TO EXTREMISM

The Internet, like an ocean that encompasses the surface, deep and dark webs (Chen et al., 2008), poses complex challenges for the fight against extremism. While terrorist groups like IS skillfully use the Dark Net and social media to spread their messages (Weimann, 2016), security forces and academia often lag behind. Academic analyzes offer deep insights into radicalization, but their application is hampered by complexity and lack of practicality (Wall, 2007). This section explores two key reasons for this failure: overcomplicated narratives that fail to reach target groups and a lack of emotional engagement and simplicity in counterattacks.

Overcomplicated Narratives: Why Academic Analyzes Fail to Reach Target Groups

Extremist messages are quick and simple, like arrows aimed at vulnerable individuals (Malik, 2018). In contrast, academic analyzes often act as cumbersome nets that cannot capture the target (Desjardins, 2019). We can consider this through several aspects.

Unrecognizability and inaccessibility for target groups. The language of academic analysis is often too technical, full of theoretical concepts that are understandable only to a specialized audience (Europol, 2017). For example, sociological-cultural studies that see marginalization as a cause of radicalization use terms like “social capital” or “collective efficacy”, which is far from the everyday experience of young people from vulnerable communities – the primary target of extremist messages (Wimmer, 2015). According to Wimmer, these groups require messages tailored to context, not abstract theories. The absence of simple language makes it impossible to directly influence individuals on the verge of radicalization.

Limited practical applicability. Theoretical frameworks often remain trapped in professional journals with a limited reach (Weimann, 2018). Even when they reach decision makers or practitioners on the ground, such as police officers or social workers, their complexity prevents implementation (Grabosky, 2017). A Europol report (2017) points out that practitioners do not have the capacity to decipher complex models, which creates a gap between theory and practice. According to Burton, while IS masterfully engages individuals, institutional responses lose ground due to over-academicization (Berton, 2015, as cited in Weimann, 2016).

Ignoring the local and cultural context. Academic analyzes often strive for universal solutions, ignoring local and cultural specificities (International Monetary Fund [IMF], n.d.). Extremism is deeply rooted in social context – a message that works in one community may be counterproductive in another (Wimmer, 2016). For example, analyzes that do not take into account ethnic tensions or religious sentiments in a particular region fail to get to the heart of the problem, making them less relevant to their target communities (Weimann, 2016).

Ignoring the influence of the digital world. In the digital era, extremists use social media, memes and viral messages to spread ideology, relying on brevity and emotion (Wimmer, 2016). Academic discourse, on the other hand, remains long and complex, hardly finding a place in this space where attention spans last eight seconds (Desjardins, 2019). Extremist content creates a sense of belonging, while academic works seem alienating, missing the opportunity to become part of a narrative that influences young people (Weimann, 2018).

Lack of interactivity. Academic publications are static and do not allow two-way communication (Wall, 2007). Target groups have questions and dilemmas that require interactivity, while extremists offer direct contact through platforms like Telegram (International Center for Counter-Terrorism [ICT], 2016). This lack of interaction further diminishes the impact of academic insights.

Lack of Emotional Engagement and Simplicity in Counterattacks

While extremists use emotions as weapons – fear, anger or pride – official counterattacks often remain sterile and devoid of force (Malik, 2018). One of the key problems of modern responses is the inability to emotionally engage the audience and simplify messages in an understandable and persuasive way.

The emotional void of the counter-narrative. Extremist messages reinforce a sense of belonging and identity, while counter-narratives ignore these emotional needs (Weimann, 2016). Institutional messages, such as "Terrorism destroys communities", rely on logic but do not touch the hearts of those whose radicalization begins with a sense of marginalization (Wimmer, 2016). A young person who feels alienated is not only looking for rational arguments, but also recognition of their emotions – which counter-narratives rarely provide (Weimann, 2018).

Complexity of messages and loss of attention. Extremists use concise slogans and short video clips that quickly attract attention (Malik, 2018). In contrast, counter-narratives often use technical language and long texts, losing competition in the digital world where attention is limited (Desjardins, 2019). Islamic State's message to "Be part of something bigger" fits into 140 characters, while institutional responses require paragraphs, making them unattractive.

Lack of authenticity. Extremist messages seem authentic because they speak directly to the experiences of the audience, often through community voices (Weimann, 2016). Counter-narratives from institutions are perceived as insincere or propaganda, especially due to the absence of local voices that would make them more believable (Malik, 2018).

Absence of cultural and local adaptation. Extremists use cultural references to increase influence, while counter-narratives remain generic and unadapted to the local context. A message adapted to Western society may be incomprehensible in collectivist cultures, which reduces its reach (Wimmer, 2016).

Focusing on punishment instead of prevention. Security responses often emphasize punishment – arrests and courts – to the neglect of empathy and prevention (Europol, 2017). This repression reinforces the sense of marginalization exploited by extremist, while positive preventive narratives are absent (Weimann, 2018).

Insufficient use of digital and creative tools. There are differences in the application of digital tools, with institutions tend to be quite conservative in this regard, while extremists use mimes and interactive formats (Weimann, 2016). This is also logical, bearing in mind that extremists want to increase the emotional reach of the counter-narrative, and this is achieved through creative approaches, e.g. short films or the inclusion of influencers (Malik, 2018).

What we usually have as answers is like fishing without the right bait – the answers are too complicated, without the emotional strength to successfully counter extremist narratives (IMF, n.d.). For a more effective fight against extremism, it is necessary to introduce simplicity, emotions and, necessarily, local context into the answers.

PROPOSING AN EFFECTIVE COUNTER-NARRATIVE

Extremist groups like IS have shown that they can successfully use Dak Net and social media for radicalization through simple and emotional narratives (Weimann, 2016). As we have stated, current responses suffer from overcomplication and lack of engagement, and an effective counter-narrative is expected to bridge this gap. It seems that the right solution could be to develop a strategy based on photos, videos and messages of up to 140 characters, which are, of course, adapted to the digital age and local contexts.

Why Simplicity Works: Psychology and Communication

Extremist messages work because they are concise and emotionally powerful, fostering a sense of belonging and purpose (Malik, 2018). As shown by some psychological studies, such messages require less cognitive effort, and this is also the reason why they reach the audience faster (Kahneman, 2011). Also, research shows that the optimal duration of attention in the digital space is eight seconds (Desjardins, 2019), and it is known in advance that complex narratives lose their impact. Therefore, the counter-narrative must be short and direct, with content from the everyday life of the target audience and, necessarily, with a positive message, which is also taken into account when creating extremist slogans.

Elements of a Successful Counter-Narrative: What to Include in 140 Characters

An effective counter-narrative should contain three key elements: emotion, authenticity and action. For example, a message like "Your voice changes the world - be part of the change" (103 characters) offers hope and inclusion, countering the extremist "Join the fight" (Malik, 2018). Photos of young people from local communities or short videos of successful reintegrations (Wimmer, 2016) reinforce the impression. These elements must be culturally adapted – what works in Indonesia may fail in the Middle East (Europol, 2017).

Examples: Specific Suggestions for Photos, Video Content and Short Messages

a) Photo: Picture of a group of young people building a park together, with the message "We are building the future together" (79 characters).

b) Video: 15-second clip about a former extremist who now runs a youth center, with the caption "My way is peace - find yours" (90 characters).

c) Message: "Your strength is in community, not in hatred" (107 characters), with a picture of a local festival.

These examples use visual power and brevity to convey a positive identity, countering extremist propaganda (Weimann, 2018). A counter-narrative of photos, videos and 140 characters can rival extremist messages if it is simple, emotional and locally relevant (IMF, n.d.). This approach requires the cooperation of institutions, communities and digital experts in order to effectively counter radicalization.

IMPLEMENTATIONS AND CHALLENGES

A proposed counter-narrative based on photos, video and messages of up to 140 characters offers a simple and emotional response to extremism (Malik, 2018). However, its implementation requires strategic distribution and faces serious challenges. Therefore, it is necessary to consider how to reach the audience and overcome obstacles in practice.

Distribution Platforms:
How to Reach an Audience on Social Media

The distribution of counter-narratives must take advantage of social networks such as TikTok, Instagram and Telegram, where extremists already operate (Weimann, 2016). Short video content and messages tailored to the algorithms of these platforms can quickly reach young people (Desjardins, 2019). For example, collaboration with local influencers on Instagram can increase the visibility of the message "Building the future together" (Wimmer, 2016). Institutions should hire digital marketing experts to ensure virality, while using paid campaigns to precisely target vulnerable groups (Europol, 2017). Quick adaptation to trends in the digital space is of great importance.

Potential Obstacles:
Legal, Technical and Ethical Challenges

Implementation faces multiple obstacles. Legal challenges include regulation of privacy and data protection on platforms, such as GDPR in Europe, which can make it difficult to target audiences without breaking the law (Wall, 2007). In terms of technical challenges, they are seen in the rapid removal and adaptation of content by extremist groups. In order to achieve this, it is necessary to change sophisticated algorithms, that is, to carry out constant technological upgrading, for which advanced IT skills are necessary (Weimann, 2019). Ethical challenges concern the risk of stigmatizing communities if messages are misinterpreted as propaganda (IMF, n.d.). For example, a video about the reintegration of ex-extremists can cause negative reactions if it is not culturally sensitive (Wimmer, 2016). In addition, campaign financing and coordination between governments, NGOs and technology companies present logistical difficulties (Europol, 2017).

Effective implementation of counter-narratives requires smart distribution and overcoming legal, technical and ethical obstacles (Malik, 2018). Success depends on flexibility, cooperation and sensitivity towards local communities in order to counter extremist propaganda on their turf.

CONCLUSION

The connection of the digital world brings many good things into people's lives, but like many other human products whose primary purpose is the welfare of humanity, it has also brought some negative phenomena, among which is opening the door for extremism to take root in a way that was not possible before. The Dark Net and social media have become tools for terrorists to spread their messages, recruit followers and plan attacks, relying on simplicity that easily finds its way to vulnerable individuals. While they build their "theatre" online, security forces and academia remain stuck in a web of overanalysis and complex strategies that fail to reach where it is most needed – the ordinary people who are the targets of these messages. This paper shows that the crux of the problem lies precisely in this gap: while extremists use darts that hit the heart, the official responses are like fishing without the right bait - too convoluted to catch the right target.

Simplicity is what gives extremists an edge. Their messages don't require much thought - they are quick, clear and full of emotion that appeals to those who feel lost or rejected. On the other hand, institutions still offer answers that are far from everyday life, full of theories and technical concepts that do not speak the language of the communities they are intended for. Herein lies the key lesson: if we want to counter radicalization, we must fight on the same ground – the digital space where everything happens, and with tools that are as fast and powerful as those wielded by extremists. Photos, videos and messages of up to 140 characters are not just a technical gimmick, but a way to bring humanity back into the fight against hate, to show that community and hope can be stronger than fear and anger.

Implementing this approach is not an easy matter. Legal obstacles, such as privacy regulations, can slow down the process, while technological difficulties require constant monitoring and adaptation to the rapid changes introduced by extremists. Ethical challenges, such as the risk of stigmatization, remind us that every step must be carefully considered, because a wrong move can only deepen the gap between communities and institutions. Funding and coordination between different actors – governments, NGOs, technology companies – further complicate matters. But that's exactly where the strength of this proposal lies: it doesn't ask for a perfect system, but flexibility and a willingness to go where the people are, to speak their language and show them something they can believe in.

Ultimately, the fight against extremism is not only about security, but also about understanding. As long as the answers remain in offices and on the pages of thick reports, extremists will have the upper hand on the ground where the real battle is being fought - in the minds and hearts of individuals. The proposed counter-narrative is not a magic wand, but it is a step towards bringing that fight back to where it belongs: to the communities that can win it, given the chance. Simplicity, emotion and local context are not just tactics – they are a way to show that there is a better way, one that leads to togetherness, not destruction.

REFERENCE LIST

Berton, B. (2015, June). *The dark side of the web: ISIL's one-stop shop*. Report of the European Union Institute for Security Studies. The Dark Side of the Web: ISIL's One-Stop Shop?

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the dark web: A case study of Jihad on the web. *Journal of the American Society for Information Science and Technology*, 59(8), 134–1359. https://doi.org/ 10.1002/asi.20838

Europol. (2017). *Internet organised crime threat assessment (IOCTA)*. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

Grabosky, P. (2017). The evolution of cybercrime, 2006-2016. In T. J. Holt (Ed.), *Cybercrime through an interdisciplinary lens* (pp. 15–36). Routledge.

International Center for Counter-Terrorism [ICT]. (2016). *Trends in the Operational Arena*. https://www.jstor.org/stable/pdf/resrep09459.4.pdf

International Monetary Fund. (n.d.). The truth about the Dark Web. https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-web-kumar.htm

International Telecommunication Union [ITU]. (2023, November 27). *New global connectivity data shows growth, but divides persist.* https://www.itu.int/en/mediacentre/Pages/PR-2023-11-27-facts-and-figures-measuring-digital-development.aspx

Jenkins, B. (1975). *International terrorism*. Crescent Publication.

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Malik, N. (2018). T*error in the Dark.* Henry Jackson Society. https://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf

Desjardins, J. (2019, March 13). *What happens in an Internet minute in 2019?* Visual Capitalist. https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age.* Polity Press.

Weimann, G. (2016). Terrorist migration to the Dark Web. *Perspectives on Terrrorism*, 10(3), 40–44. https://www.jstor.org/stable/26297596?seq=1

Weimann, G. (2018, April 27). *Going darker? The challenge of Dark Net terrorism.* Wilson Center. https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_terrorism.pdf

Wimmer, A. (2016). *Dark net, social media and extremism: Addressing Indonesian counter-terrorism on the Internet*. Academia.edu. https://www.academia.edu/20813843/Dark_net_Social_Media_and_Extremism_Addressing_Indonesian_Counter_terrorism_on_the_Internet

Zirojević Fatić, M. (2011). Zloupotreba interneta u svrhe terorizma [Abuse of the Internet for terrorist purposes]. *Međunarodni problemi*, 63(3), 417–448.

***Dijana Vučković*[1]**
***Veselin Mićanović*[2]**

ETHICAL COMPETENCES FOR THE USE OF ARTIFICIAL INTELLIGENCE IN EDUCATION

Abstract

Digital technology has brought numerous opportunities but also challenges in teaching and learning. Some of these challenges are particularly relevant in the context of preserving academic integrity. The rapid development of artificial intelligence further emphasizes the necessity of ethical education, as the opportunities available to students and other individuals in academia can be jeopardized if not used in an ethical manner. The Council of Europe, OECD, and UNESCO highlight the importance of the ethical dimension in education through their conventions and competency models for the use of artificial intelligence. The Council of Europe has published a convention focused on the protection of human rights in the era of artificial intelligence, UNESCO has developed competency models for teachers and students, and the OECD has produced various documents regulating the use of artificial intelligence. The goal of this work is to provide a comprehensive overview of the ethical dimension of education in the relevant reports, conventions, and competency models of the mentioned organizations. Our research question is: What ethical competencies are directly related to the use of artificial intelligence? We sought to answer this question using theoretical analysis, which includes a description of ethical competencies and their levels, with particular emphasis on UNESCO's competency models. Based on this analysis, we propose necessary implications for university teaching practice. In other words, based on the results of this desk research, we have created recommendations that could enhance the ethical component of teaching and learning in academia in the era of AI.

Keywords: *Academic Integrity, Ethical Competencies, Competency Models, Teacher, Artificial intelligence.*

INTRODUCTION

Artificial Intelligence (AI) represents the most important technological revolution of modern society. Its application in teaching, learning, and research, as well as in the entire academic sector, opens numerous opportunities for improving educational

[1] Faculty of Philosophy, University of Montenegro, Podgorica, Montenegro, dijanav@ucg.ac.me

[2] Faculty of Philosophy, University of Montenegro, Podgorica, Montenegro, veselinm@ucg.ac.me

and research processes. Furthermore, AI has capabilities that could certainly handle vast amounts of administrative tasks. AI is already present in many areas of education, from personalized learning that adapts to the needs of each student, thereby fulfilling the didactic principle of individualization like never before, to automated systems that assist in the analysis of large amounts of data.

Although AI brings numerous advantages and presents almost unimaginable possibilities, it must be kept in mind that its use also carries risks related to ethical dilemmas and data privacy issues. The development and application of AI in education is, therefore, not only a technological challenge, and it is not enough to simply train users for its use in this sense, but it is also an ethical issue, because each advancement requires a new level of responsibility. Academic integrity is a necessary prerequisite in the academic community, as its respect preserves the quality and reliability of the educational system, and aims to prevent the unethical use of technologies (Cotton, Cotton & Shipway, 2023). The implementation of AI must be subject to strict ethical standards that will ensure it is used in accordance with the values of the academic and wider social community, such as respect for human rights, justice, and integrity.

The goal of this paper is to analyze the ethical principles and competencies for using AI, which have been developed by organizations such as UNESCO, the Council of Europe, and the OECD. At the end of the paper, recommendations are provided that higher educational institutions (HEIs) can currently use for the safe and functional implementation of AI in teaching and learning processes.

OPPORTUNITIES AND ETHICAL DILEMMAS OF USING AI IN EDUCATION

AI and generative AI technology are rapidly developing and are recognized as key factors in transforming the education sector. The use of AI in teaching could dramatically improve the quality of education, allowing teachers to focus more on creative and interactive aspects of teaching, as well as on meaningful interactions with their students and colleagues, while AI takes on administrative tasks and provides personalized approaches to learning. However, AI also brings numerous challenges, and it is important to consider these when integrating AI into educational systems. In both academic and broader societal communities, there is a need to clearly define norms and guidelines for its responsible application.

OECD, reflecting on the potential ethical challenges of AI use, states:

> AI actors should respect the rule of law, human rights, democratic and human-centred values throughout the AI system lifecycle. These include non-discrimination and equality, freedom, dignity, autonomy of individuals, privacy and data protection, diversity, fairness, social justice, and internationally recognised labour rights.

> This also includes addressing misinformation and disinformation amplified by AI, while respecting freedom of expression and other rights and freedoms protected by applicable international law. To this end, AI actors should implement mechanisms and safeguards, such as capacity for human agency and oversight, including to address risks arising from uses outside of intended purpose, intentional misuse, or unintentional misuse in a manner appropriate to the context and consistent with the state of the art. (OECD, https://oecd.ai/en/dashboards/ai-principles/P6)

Therefore, it is evident that a human-centered approach and ethical use of AI must be prioritized, as otherwise, there is a risk of violating human rights and even undermining the fundamental principles of democracy itself.

Bit, Biwas and Nag (2024) explored the impact of artificial intelligence (AI) on education, highlighting its benefits and challenges. AI technologies such as natural language processing and machine learning can personalize learning, improve administrative efficiency, and increase student engagement. Benefits include tailored educational experiences, intelligent tutoring systems, data-driven insights, and increased accessibility for students with disabilities. AI also streamlines administrative tasks and supports collaboration between teachers and students. Challenges include concerns about privacy, potential biases, over-reliance on technology, cost differences, job loss, and ethical questions. A balanced approach is needed to maximize the benefits of AI while addressing these challenges (Bit, Biwas & Nag, 2024).

AI will certainly be applied in different ways across various fields of study. Below, we consider several potential general benefits that AI could bring to studies:

a. Improved Learning Experience through Personalization

AI enables personalized learning that adapts to the needs of each student (Feng, 2025). This concept essentially represents the fulfillment of the long-established principle of individualization in teaching, which didactics has never fully achieved. In the age of AI, by using intelligent tutoring systems and learning platforms, students can learn at their own pace, potentially increasing efficiency and motivation, although not necessarily, as social interaction and peer learning have important motivational benefits. Students with different learning styles can receive appropriate resources and support, enabling them to master the material in the best way.

b. Simplified Research Processes

AI-based tools such as Semantic Scholar allow researchers to more easily search and analyze literature (Razack et al., 2021). AI can shorten the time needed to study large amounts of academic papers. Moreover, AI can automatically summarize relevant information, helping researchers focus on the most important aspects of their research. This could potentially accelerate the discovery of new insights.

c. Fast and Efficient Data Analysis
In scientific disciplines that require, for example, statistics or any other large-scale data analysis, AI can process unimaginable amounts of data quickly (Ivanović, 2023). In the social sciences, for example, AI is used to analyze data from social networks and surveys, enabling a better understanding of public opinion and social changes. In educational research, AI can also process large amounts of data and, for instance, provide almost perfect learning analytics.

d. Enhanced Peer Review and Other Forms of Evaluation
AI plays a key role in the academic peer review process, where it can detect plagiarism, suggest reviewers, and even assess the quality of submitted papers. In teaching, following the same principle, AI can quickly and efficiently review students' work and provide valid and comprehensive feedback (Chang et al., 2023).

Given that AI can imitate human intelligence and process data faster and more accurately than humans, its potential in education is immense. For instance, AI can analyze student performance and difficulties in real-time, providing teachers with data that allows them to better tailor their teaching to each individual (Feng, 2025; Ivanović, 2023). Additionally, AI helps in self-regulating the learning process (Chang et al., 2023), as well as in evaluation and grading (Ding & Zou, 2024). However, the benefits of AI also come with significant challenges – ethical issues, data privacy concerns, and risks of over-reliance on technology that could reduce human creativity and critical thinking, meaning educational institutions must develop a balanced approach to AI usage (Cacho, 2024). Below are some identified risks:

a. Ethical Dilemmas
AI systems can express biases, even prejudices and stereotypes that exist in the data on which they are based (Ozkul, 2024; Zhou & Kawabata, 2023). For example, Ozkul (2024) points out that AI-produced technologies can produce discriminatory and biased results or analyses based on ethnicity, religion, and gender. Such biases towards certain social groups naturally raise concerns about fairness and transparency in AI use. Discrimination and bias in AI algorithms are based on the data used to train them, and this data may contain consciously or unconsciously produced prejudices or be biased. For example, if AI is used to select candidates for certain scholarships, the algorithm may unintentionally favor specific student groups based on data that does not reflect fairness (e.g., students from particular geographic areas, countries, ethnic groups, social classes, etc.). This type of bias can lead to increased inequality in educational systems and exacerbate existing social and economic differences.
The crucial question here is: According to which ethical norms and values does AI operate? In many cases, AI systems are developed in the context of specific

cultural and societal norms that may differ from those in educational systems of other countries. AI simply generates data collected from the internet, but not all societies participate equally in the production of internet content. For example, algorithms used to assess students, such as automated essay grading systems, may be insensitive to cultural differences in language and writing style, which can lead to inaccurate and unfair assessments. Or, if an algorithm uses pre-defined criteria that do not take into account creativity or originality, students who think outside the box may be unfairly graded. Additionally, it is important to consider how AI is used to create personalized learning experiences—whether the algorithms suggesting learning content are truly based on a general, balanced approach, or if they favor specific perspectives, strategies, techniques, and methodologies, thereby neglecting diversity in learning approaches.

b. Over-reliance on AI
If we become overly reliant on AI for grading or decision-making, it may result in reduced human creativity and critical thinking. While AI can automatically generate grades or decisions, the human factor in education is still crucial for understanding context and making moral decisions. Additionally, excessive reliance on AI can undermine students' ability to develop critical thinking and even their ability to learn through more complex forms of learning that depend on insight-based learning.

c. Privacy and Data Protection
AI systems that process sensitive data must comply with regulations regarding data protection. In the academic environment, where data about students, researchers, and teachers is processed, it is important to implement secure systems to prevent unauthorized access to data. The set of data collected in academic institutions may include information about students' abilities, learning preferences, grades, and other personal factors. Using this data to personalize learning can be useful, but it can also create opportunities for misuse. Furthermore, there are ethical concerns regarding data ownership – who owns the data that AI systems collect: students, educational institutions, or the companies that develop the AI technology?

d. Job Loss
The automation of administrative and teaching tasks may lead to job reductions, which raises concerns for many academic institutions. Institutions should invest in staff retraining to adapt to new technologies and ensure that jobs remain relevant in the AI era. One of the most concerning ethical challenges from the perspective of pedagogical-psychological and other educational sciences is the potential automation of educational processes, which could lead to reduced human engagement and, in some cases, even complete replacement of teachers by AI systems. From the perspective of educational sciences, this would make no sense, as social

constructivism, as the leading learning paradigm, clearly indicates that educational goals are far broader than cognitive learning outcomes, and issues related to the development of students' personalities in emotional, moral, social, etc., terms cannot be addressed without human interaction. AI can be an effective tool for administrative tasks in education, such as grading and tracking student progress, but it should not be considered as a replacement for teachers. Quality education is based on social and emotional interaction, which AI cannot provide. For instance, AI can analyze data about a student, but it cannot recognize the emotional or psychological needs of the student in the same way a teacher can.

Given the truly unprecedented opportunities that AI offers to universities for teaching and learning in the AI era, it is crucial to constantly be mindful of the ethical application of this advanced technology. Key areas requiring attention include data privacy protection, fairness in algorithm application, reducing human engagement to prevent job loss, and continuously updating appropriate ethical guidelines to ensure that AI is used in accordance with human rights and academic integrity principles.

ETHICAL DIMENSION OF AI USE IN RELEVANT INTERNATIONAL DOCUMENTS

EU Regulation 2024/1689 sets a framework for the ethical development and application of AI within the European Union. The goal of this document is to ensure transparent, fair, and responsible management of AI technologies, while respecting human rights and freedoms. AI systems created or used within the EU must comply with human rights, such as the right to privacy and freedom of expression, with an emphasis on preventing any discrimination or inequality among users, regardless of their personal and identity characteristics such as race, gender, or disability.

The leading principles of Regulation (Uredba, 2024) are transparency and accountability, implying that users and authorities must have a clear understanding of how AI systems operate and how they make decisions that affect their lives. Providers of AI systems should be held accountable for any misuse or errors the system may cause. Furthermore, the Regulation (2024) insists that human control must be present in all key decisions made by AI systems, especially concerning high-risk activities such as healthcare, justice, and employment.

User safety is, among other things, a priority, and AI systems, especially those that may present high risks, must undergo rigorous testing and certification to ensure their safety and prevent potential physical or mental harm to users. User privacy must be protected in accordance with data protection laws, and all data related to AI systems must be collected and processed legally.

Regulation (2024) also emphasizes social responsibility and sustainability, highlighting that AI technologies must contribute to positive social, economic, and ecological changes, rather than creating a wave of negative changes. It is important to ensure equal access to AI technologies for all EU citizens in order to prevent social inequality. The Regulation provides for continuous monitoring and revision of AI systems to ensure their alignment with ethical principles and appropriate laws.

The AI Act, discussed in March 2024 at the Plenary of the European Parliament (P9_TA(2024)0138 Artificial Intelligence Act), presents vital information for those involved in the development or application of AI technologies in the EU. This law aims to establish a regulatory framework that ensures the safety and protection of citizens while also encouraging innovation. The law is designed to minimize or completely eliminate the potential risks AI may pose to human rights and safety, while simultaneously enabling the competitiveness and development of this technological sector.

The law regulates all AI systems used within the EU and directs them towards a clear classification of potential risks. Based on this classification, AI systems that present a higher risk level are subject to strict regulations and enhanced oversight, while certain systems that pose unacceptable risks, such as biometric recognition in public spaces, are strictly prohibited. Providers of AI systems are responsible for product safety, and the law requires them to take measures for risk assessment and to enable monitoring of technology deployment. Transparency and the ability to audit AI systems are also mandatory (AI Act, 2024).

Although the law sets strict and sometimes rigorous rules, it simultaneously encourages innovation and competitiveness within the AI industry, aiming to position the European Union as a global leader in the responsible application of AI. For all providers and implementers of AI technologies, this document is crucial as it offers guidance on how to align their operations with legislation and ensure that AI systems are safe, ethically acceptable, and in compliance with legal norms.

The law particularly emphasizes the ethical aspects of AI application, including user rights protection and the prevention of discrimination. The goal is to ensure that AI systems do not infringe on human rights, such as privacy, freedom of speech, and the right to a fair trial. Within the law, ethical principles are key to shaping the legislative framework that will govern the development and application of AI in the EU. These principles aim to ensure that AI systems do not endanger the safety, freedoms, and rights of citizens but instead contribute to their well-being and positive social change.

The leading ethical principles of the AI Act by the European Commission (2024) are:

– Transparency and Accountability. Providers and users of AI systems must be able to clearly explain how their AI systems function, including an explanation of the methodology used. AI systems must also be designed in a way that enables accountability in the event of errors or harmful consequences.

– Ban on Discrimination. The AI Act has established frameworks to prevent any discrimination that AI systems might cause. The EU implements a policy of equality and non-discrimination, and all AI systems are expected not to make decisions that favor or discriminate against any individual or group based on race, gender, age, sexual orientation, disability, or other personal characteristics.
– Respect for Privacy and Data Protection. Since many AI systems use personal data to learn and make decisions, protecting privacy becomes crucial in the era of AI. The law is aligned with the General Data Protection Regulation (GDPR) and ensures that all AI technologies comply with the highest data protection standards.
– Human Control and Autonomy. The AI Act emphasizes human control in the decision-making process. Since AI can make decisions based on available data and algorithms, it is important that humans still have control over significant decisions, especially those that have a vital impact on people's lives.
– Safety and Security. AI systems must be designed in a way that does not jeopardize the physical and mental safety of users. For this reason, the law insists that all high-risk AI systems must undergo rigorous safety testing and that providers must continuously monitor system operations to detect potential problems in a timely manner.
– Access and Equality. The law also promotes inclusiveness in the application of AI technologies, ensuring equal access to AI for all EU citizens, who should have equal opportunities to use AI products and services.

These principles are not merely abstract guidelines but are concretely embedded in legislative regulations that define the obligations of providers, implementers, and end users of AI technologies. They are also foundational to building trust in AI technologies. They should enable individuals and society to trust that AI will contribute to positive changes without infringing on their fundamental rights and freedoms, and without posing a threat to safety.

The Council of Europe *Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law* (Council of Europe, 2024), based on the Council of Europe's *Explanatory Report to the Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law* (2024), is a framework document that seeks to guide the development and application of artificial intelligence in Europe from an ethical standpoint, while respecting fundamental human rights, democracy, and the rule of law. Given that AI technology is increasingly shaping society, the Council of Europe considers it crucial to ensure that the use of AI systems complies with legislation that protects human welfare.

One of the key objectives of this Convention is the protection of human rights. This includes the right to privacy, freedom of speech, and the right to a fair trial, with a particular focus on ensuring that AI systems do not undermine any of these fundamental rights. In developing guidelines for the ethical use of AI, the Convention stresses that it is necessary for AI technologies to operate in accordance with the fundamental values of society and to respect the integrity and safety of each individual.

Additionally, the Convention calls for transparency regarding how AI makes decisions. This means that users and authorities should have the ability to understand how AI systems function and based on which data decisions are made. This is particularly significant to avoid situations where people might be subjected to unjust or incomprehensible decisions made by AI systems.

The Council of Europe also highlights the importance of international cooperation among member states. Only through joint efforts and the exchange of best practices can global standards be created to ensure the responsible application of AI across various sectors, including education, healthcare, law, security, and the economy. Essentially, like documents created by the European Commission, this Convention seeks to balance technological progress with the preservation of human values, ensuring that AI is a technology or tool that contributes to the welfare of society rather than a threat to its foundations.

UNESCO'S COMPETENCY FRAMEWORKS FOR AI USE BY TEACHERS AND STUDENTS

UNESCO has played a key role in shaping a global ethical strategy for the use of AI, especially in education. They have developed guidelines and reference competency models focusing on how to use AI in a way that is safe, fair, beneficial for individuals, and society (UNESCO 2024a; 2024b). The key principles in UNESCO's models for AI usage include: the protection of human rights and dignity, access to education and reducing inequality, transparency and accountability, applying ethics in design and implementation, and AI education.

UNESCO's competency models for teachers and students (UNESCO 2024a; 2024b) offer educational guidelines based on understanding the ethical, social, and cultural aspects of using AI technologies. These models aim to balance technological progress with the need for responsible and ethical management of this technology. This is of particular importance for academic communities that wish to integrate AI into the teaching process. Essentially, students and teachers already use AI, but they do so without clear rules or limitations. Higher education institutions should adopt standards and guidelines for the responsible use of AI as early as possible (U.S. Department of Education, Office of Educational Technology, 2023). This also includes the development of competency models necessary for students, teachers, and researchers to use AI effectively.

The UNESCO AI Competence Frameworks for both teachers and students (2024a; 2024b) are clear, well-structured, and deeply thought-out documents created with the intent to provide guidelines on how AI can be integrated into teaching and learning.

What is particularly significant in this work is that both UNESCO models place a strong emphasis on ethical AI usage because “AI may threaten human agency, intensify climate change, violate data privacy, deepen long-standing systemic inequalities and exclusion, and lead to new forms of discrimination” (UNESCO, 2024b, p. 13).

UNESCO emphasizes that AI must inevitably be integrated into the communication between teachers and students, which it already is. This applies to all educational systems, although only a few have defined competencies or rules for AI usage. Both competency frameworks (for students and teachers) developed by UNESCO are based on the same methodological principles and have many common features, but they are not identical (UNESCO 2024a, 2024b). The framework for teachers covers 5 competency aspects defined across three levels of progression, making a total of 15 competency groups, while the framework for students also includes three levels of progression but for 4 aspects, totaling 12 groups. Two aspects have the same name in both frameworks: a human-centered approach and ethics of AI usage, but their specific competencies differ depending on whether the individual is a student or teacher (UNESCO 2024a, 2024b).

The aspect called Human-Centered Mindset is highlighted in both models, focusing on human agency and responsibility. (In addition to a human-centered approach, it might be suggested to add a nature-centered mindset, keeping in mind the principles of sustainable development). AI should be viewed as a technology that complements and helps accelerate human abilities rather than replaces or diminishes them. It is encouraging that UNESCO emphasizes this aspect, and according to the given models, both students and teachers should understand the implications of their interactions with AI and actively ensure that it serves humanity in ethical ways. Furthermore, “Values of empathy, altruism, justice, intercultural compassion and solidarity are essential for social cohesion and to uphold our common humanity. AI and other digital technologies must not discourage people from staying in contact with others and with the real world, as well as from respecting rights to ways of living and knowing beyond digital spaces” (UNESCO, 2024b, p. 16).

The aspect called Ethics of AI also appears in both UNESCO competency models. This aspect – which is directly related to the previous one – forms the core of the competency models (UNESCO 2024a; 2024b). Naturally, the elaboration of this aspect differs for teachers and students. For teachers, the focus is on creating a safe and responsible learning environment that includes AI technology, with the addition that teachers should contribute to the creation of ethical guidelines. Essentially, as AI advances, new ethical dilemmas will arise, making it particularly important for teachers to learn how to guide students through complex moral challenges. Therefore, teachers may experience a shift in their roles in an AI-driven learning environment, from being the content deliverer (a role AI might perform to some degree) to being those who focus on ethical principles and training students to respect those principles. Ethical principles such as data privacy, inclusivity, and sustainability are essential components for both students and teachers.

As already mentioned, the competencies are set at three proficiency levels (Table 1, Table 2). The first progression level in both models includes knowledge, skills, and attitudes related to artificial intelligence at a basic level, the second covers practical skills and the flexible application of AI, while the third level focuses on creating and evaluating content using AI. This hierarchical organization of levels is aligned with Bloom's taxonomy for the cognitive domain.

The competencies for teachers are defined across three levels of progression: acquisition, deepening, and creation (UNESCO 2024b).

Table 1. *Competency Framework for Teachers: Aspects and Levels of Progression*

Aspects	**Progression**		
	Acquire	Deepen	Create
Human-centered mindset	Human agency	Human accountability	Social responsibility
Ethics of AI	Ethical principles	Safe and responsible use	Co-creating ethical use
AI foundations and applications	Basic AI techniques and applications	Application skills	Creating with AI
AI pedagogy	AI-assisted teaching	AI-pedagogy integration	AI-enhanced pedagogical transformation
AI for professional development	AI enabling lifelong professional learning	AI to enhance organizational learning	AI to support professional transformation

Source: UNESCO AI competence framework for teachers (2024b, p. 22)

Five Aspects of Competencies for teachers are: Human-Centered Approach, AI Ethics, Fundamentals and Applications of AI, Pedagogy of AI, and AI for Professional Development (Table 1). These aspects are deeply interconnected, and each one has its own internal coherence. Each of them is formulated in terms of knowledge, skills, attitudes, and values as elements of learning and teaching. The ethical aspect, as already mentioned, emphasizes fundamental ethical principles, rules, institutional regulation, as well as practical ethical codes that teachers must adhere to. For teachers, this aspect involves progressing in understanding the ethical use of AI, skills for creating safe and responsible use of AI in an appropriate learning environment, as well as competencies necessary for developing and maintaining ethical norms (UNESCO, 2024b).

The first level (acquisition) of AI ethics for teachers involves having a deep understanding of ethical issues related to AI, as well as those encompassing the ethics of communication between humans and AI. This inevitably includes the protection of human rights, human agency, linguistic and cultural diversity, inclusive principles, and environmental protection (UNESCO, 2024b).

The second level (deepening) of ethical competencies for teachers relates to the safe and responsible use of AI in education. Teachers are expected to internalize ethical norms regarding safety and responsibility in the use of AI. These and other similar competencies must be an integral part of the norms across all phases of the educational process, including evaluation and assessment (UNESCO, 2024b).

The third level of this competency aspect for teachers focuses on updating and refining rules, which will be necessary due to the rapid development of AI technology. Thus, teachers' competencies are geared toward critical thinking, leading discussions, and activities related to ethical, sociocultural, and ecological issues. Given the rapid advancement of AI, it is expected that the process of updating ethical rules will be intense and continuous (UNESCO, 2024b).

The three levels of ethical development for teachers make sense because they ensure that teachers evolve with the technology. In addition to awareness of AI ethics, teachers should also be proactive when it comes to creating and enforcing those ethical boundaries.

Table 2. *AI competence framework for students*

Aspects	**Progression**		
	Understand	Apply	Create
Human-centered mindset	Human agency	Human accountability	Citizenship in the era of AI
Ethics of AI	Embodied ethics	Safe and responsible use	Ethics by design
AI techniques and applications	AI foundations	Application skills	Creating AI tools
AI system design	Problem scoping	Architecture design	Iteration and feedback loops

Source: UNESCO AI competence framework for students (2024a, p. 19)

The Ethical Aspect of AI for Students refers to the ethical judgments, reflections, and socio-emotional competencies that are necessary for students to understand, practically apply, and participate in adopting the rapidly growing normative framework for the use of AI. Students are expected to internalize ethics towards AI, which implies respecting human rights, justice, inclusion, equality, and other democratic values. Such ethics are based on the following principles: do no harm, proportionality in assessing AI use in a given context, non-discrimination, sustainability, transparency and explainability, safe and responsible use, and ethics by design (UNESCO, 2024a). However, the cornerstone of safe AI use is “Critical thinking is a fundamental skill that students need to meaningfully engage with AI as learners, users and creators” (UNESCO, 2024a, p. 14).

The first level of competencies for students (understanding) refers to internalized ethics and implies that students can critically understand ethical issues related to AI, taking into account all the reference groups of concepts that need to be respected, such as human rights, justice, social equality, inclusion, climate change, etc. At this first level, the principles are: do no harm, proportionality, non-discrimination, human determination, and transparency (UNESCO, 2024a).

The second level, called safe and responsible use, relates to competencies that enable students to use AI responsibly. Students must also be aware of the existing risks associated with the use of AI, such as privacy protection risks. Additionally, students should be competent to take all necessary measures to ensure that their data is collected, shared, processed, and stored in ethically acceptable ways. At this level, the safety of student-users and their peers is also of significant importance (UNESCO, 2024a).

The third level (creation) relates to the competencies of creating and evaluating materials with the help of AI, as well as adopting and assessing regulations on AI.

The UNESCO competency frameworks complement the core principles of the Council of Europe’s Convention (2024): respecting human dignity and individual autonomy, ensuring equality and non-discrimination, respecting privacy and the protection of personal data, enabling transparency and oversight, accountability, reliability, and ensuring safe innovations.

For students, the progression from embodied ethics to safe and responsible use to ethics by design is important because students need to internalize the ethical principles before they can apply them and eventually design systems in a responsible way.

Both frameworks align well with broader global principles outlined by organizations such as the Council of Europe and the OECD (2019; 2024). Principles such as human dignity, non-discrimination, and privacy protection are core to the ethical use of AI and ensuring its positive impact on society. This alignment shows UNESCO’s commitment to ensuring that AI is not only effective in education but also contributes to social good and fairness.

These UNESCO frameworks provide a solid foundation for incorporating AI into educational systems. They not only address the technical and pedagogical aspects of AI but also emphasize the importance of ethics, human rights, and accountability, which are essential for ensuring that AI serves the public good. By promoting responsible AI use and developing ethical competencies among teachers and students, UNESCO is setting the stage for a future where AI enhances education while upholding key moral principles.

CONCLUSION AND RECOMMENDATIONS

Digital technologies, including the internet and AI, continuously raise new questions related to ethics and the responsible use of technology. In the context of education, ethical guidelines become even more important in order to preserve academic integrity. The use of AI in education should be guided by deep ethical principles, which include respect for human rights, data protection, and responsible use of technology. To prevent the misuse of AI, it is necessary to develop clear guidelines and regulations that will ensure that the technology is used in a way that contributes to the improvement of education, rather than diminishing its quality.

From the previous analyses, the need for constant oversight and updating of ethical guidelines is evident, as well as their incorporation into the ethical standards of higher education institutions. With the constant progress in the field of AI, educational institutions and policymakers must continually work on updating ethical codes and regulations related to the application of AI. For instance, as technology advances, new ethical insights must be developed, along with the updating of data privacy protection procedures and the fight against bias. Continuous updates to ethical guidelines must be based on an ongoing dialogue between teachers, students, decision-makers, and creators of educational policies and standards, as well as those who develop AI technologies.

The analysis of *Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations* (U.S. Department of Education, Office of Educational Technology, 2023) points out that AI will undoubtedly influence the emergence of:

– Hybrid Learning Environments: AI will likely play a key role in the evolution of hybrid learning environments, where students can engage with materials both online and offline.

– Lifelong Learning: AI can support the trend toward lifelong learning by providing personalized education pathways for professionals who need to continuously update their skills in a rapidly changing job market.

– AI-powered Institutions: Some universities may even explore fully AI-powered or hybrid institutions that leverage AI to optimize teaching, learning, research, and administration.

All these guidelines, analyses, ideas, and current knowledge, which include assumptions for the future, must be accompanied by deep ethical reasoning based on respect for ethics and human rights. Therefore, competence models, such as those analyzed in this paper, must become an integral part of the regular training of teachers and students as soon as possible.

The analysis of *Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations* (U.S. Department of Education, Office of Educational

Technology, 2023, p. 53–60) presents the following recommendations: Emphasize Humans in the Loop, Align AI Models to a Shared Vision for Education, Design Using Modern Learning Principles, Prioritize Strengthening Trust, Inform and Involve Educators, Focus R&D on Addressing Context and Enhancing Trust and Safety, and Develop Education-Specific Guidelines and Guardrails.

Thus, AI technologies are advancing at an extraordinary rate and are already being utilized by both teachers and students, often without clear guidelines and likely without deeper reflection on possible ethical dilemmas. It is clear that AI systems can offer a lot to the education sector; they can practically solve some issues that didactics has "dreamed" of for centuries but could not address in a traditional learning environment, such as issues related to individualization or personalized learning. In this sense, AI represents an opportunity that would likely enhance learning and research processes. However, the use of such sophisticated and powerful technology brings serious challenges, especially in the ethical domain. Therefore, it is reasonable to expect that higher education institutions will begin to develop guidelines for the use of AI in teaching, learning, and research, and that in these guidelines, a human and nature-centered mindset, along with AI ethics, will be dominant and pervasive principles.

REFERENCE LIST

Artificial Intelligence Act (2024). Regulation (EU) 2024/1689, *Official Journal of EU,* Brussels: European Union.

Bit, D., Biwas, S. & Nag, M. (2024). The Impact of Artificial Intelligence in Educational System. *International Journal of Scientific Research in Science and Technology*, 11(4), 419–427, https://doi.org/10.32628/IJSRST2411424

Cacho, R. (2024). Integrating Generative AI in University Teaching and Learning: A Model for Balanced Guidelines. *Online Learning*, 28(3), https://doi.org/10.24059/olj.v28i3.4508

Chang D. H., Lin M. P. C., Hajian S. & Wang Q. Q. (2023). Educational design principles of using AI chatbot that supports self-regulated learning in education: Goal setting, feedback, and personalization. *Sustainability*, 15(17), 12921. https://doi.org/10.3390/su151712921

Cotton, D. R. E., Cotton, P. A. & Shipway, J. R. (2023). Chatting and cheating: Ensuring academic integrity in the era of ChatGPT. *Innovations in Education and Teaching International,* 60(2), 228–239. https://doi.org/10.1080/14703297.2023.2190148

Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024). Strasbourg, Council of Europe.

Ding L. & Zou D. (2024). Automated writing evaluation systems: A systematic review of grammarly, Pigai, and criterion with a perspective on future directions in the age of generative artificial intelligence. *Education and Information Technologies*, 29, 14151–14203. https://doi.org/10.1007/s10639-023-12402-3

Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, *Democracy and the Rule of Law* (2024). Strasbourg, Council of Europe.

Feng, L. (2025). Investigating the Effects of Artificial Intelligence-Assisted Language Learning Strategies on Cognitive Load and Learning Outcomes: A Comparative Study. *Journal of Educational Computing Research*, 62(8), 1961–1994. https://doi.org/10.1177/07356331241268349

Ivanović, I. (2023). Can AI-assisted Essay Assessment Support Teachers? A Cross-Sectional Mixed-Methods Reasearch Conducted at the University of Montenegro. *Annales – Series Historia et Sociologia*, 33(3), 571–590. https://doi.org/10.19233/ASHS.2023.30

OECD (2019). *AI Principles*. https://oecd.ai/en/dashboards/ai-principles/P6

OECD (2024). *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449

Ozkul, D. (2024). Artificial Intelligence and Ethnic, Religious, and Gender-Based Discrimination. *Social Inclusio*n, 12, Article 8942. https://doi.org/10.17645/si.8942

Razack H.I.A., Mathew S.T., Saad, F.F.A. & Alqahtani, S.A. (2021). Artificial intelligence-assisted tools for redefining the communication landscape of the scholarly world. *Science Editing*, 8(2), 134–144. https://doi.org/10.6087/kcse.244

U.S. Department of Education, Office of Educational Technology (2023). *Artificial Intelligence and Future of Teaching and Learning: Insights and Recommendations*. Washington, DC.

UNESCO (2024a). AI competency framework for students. Paris, UNESCO.

UNESCO (2024b). AI competency framework for teachers. Paris, UNESCO.

Uredba (EU) 2024/1689 Europskog Parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji). OJ EU 2024. Brussels: European Union.

Zhou, Y., & Kawabata, H. (2023). Eyes can tell: Assessment of implicit attitudes toward AI art. *I-Perception*, 14(5). https://doi.org/10.1177/20416695231209846

Ayfer Genc Yilmaz[1]

THE EUROPEAN UNION (EU): FROM CLIMATE SECURITY TO ECOLOGICAL SECURITY?

Abstract

This paper examines the evolution of the EU's approach to the climate-security nexus, tracing its shift from a traditional climate security discourse to an emerging ecological security perspective. By analyzing EU documents, legislations, and policies, this research reveals a growing emphasis on biodiversity, resilience, and the fight against environmental crime, indicating a potential move towards an ecocentric approach. The central question is whether the EU's engagement with environmental crime signals a genuine shift from a climate security to an ecological security perspective in practice. While the EU has made strides in acknowledging the security implications of environmental degradation, challenges remain in fully recognizing ecosystems as referent objects. This paper further explores the blurring borders between human, state and ecosystem security. The paper argues that a complete transition to ecological security requires prioritizing the well-being of the planet as a core security concern.

Keywords: *European Union, ecological security, climate security. environmental crime.*

INTRODUCTION

Since the 2000s, the changing climate has been increasingly recognized internationally as a security risk (Brown et al., 2007). In 2007, the UN Security Council declared climate change a security issue. A year later, the EU emphasized the security implications of climate change, identifying it as a 'threat multiplier' that exacerbates existing threats in various fields.[2] While the relationship between climate change and security remains debated,[3] international organizations have intensified their efforts to implement effective policy tools to mitigate its effects and safeguard both human and state security.

A recent policy paper from Carnegie Europe suggests that the EU should transition from its current concept of climate security to a more ambitious notion of eco-

[1] Istanbul Ticaret University, Istanbul, Turkey, ayfergenc@gmail.com

[2] The concept of threat multiplier refers to a climate security problem that directly affects many structures and actors from individuals to society and even states.

[3] Scholarly studies have brought a more critical perspective to the relationship between climate change and security. For a critical perspective to the relationship between climate change and security, see (Abrahams & Carr, 2017; Koubi, 2019; Theisen et al., 2013).

logical security (Lazard, 2021, p. 3). Based on McDonald's ecological security concept, this perspective advocates that securitization efforts should focus on ecosystems, instead of humans or states. Concurrently, the United States Intelligence Community, in its Annual Threat Assessment Report, highlighted the link between ecological degradation and security, labeling nature a national security issue (Office of the Director of Intelligence 2023, p. 22-25). The World Economic Forum ranks biodiversity loss and ecosystem collapse as the third-largest global risk over the next ten years, behind extreme weather events and disruptive shifts in Earth systems (World Economic Forum, 2024). A scientific study revealed that biodiversity loss is the biggest environmental driver of infectious disease outbreaks, a fundamental threat to global health (Weston, 2024).

By focusing on the concept of ecological security, I aim to determine whether the EU intends to shift from a climate security discourse to an ecological security discourse. Benjaminsen (2022), criticizing Mcdonald's concept, notes that it lacks a clear articulation of what ecological security looks like in practice. This paper, therefore, asks whether the EU has the appropriate mechanisms to implement an ecological security perspective. Significantly, could EU-led efforts to address environmental crime serve as a catalyst for this transition from climate to ecological security? Specifically, this study investigates whether the EU's actions against environmental crime represent a practical shift toward an ecological security discourse (McDonald, 2018, p. 174).

This research employs an interpretative research design. For data collection, I relied on a qualitative approach and used document-based research. The focus lies on the environmental security discourse within EU policy documentation. I conduct a document review of EU documents, legislation, strategies and action plans. This design enables an in-depth exploration of meanings and underlying assumptions in the EU discourse. Focusing on EU documents, legislations, strategies, and action plans ensures access to primary sources directly shaping environmental security policy. For data analysis, the paper relies heavily on discourse analysis, a critical and interpretive method. When analyzing data, I search for keywords such as environmental degradation, biodiversity, ecology and concentrate my research on the intersection of the environment-related concepts with security.

The paper proceeds in three stages. First, I explore the differences between climate security and ecological security, focusing on McDonald's suggestion to adopt an ecological security perspective for a more comprehensive understanding of the environment-security relationship. In the same section , I also explore the concept of environmental security to establish clear differences and analyze their respective implications for human and state security. Second, I examine the historical development of the EU's climate security discourse and the evolution of the term "climate change" in light of efforts to expand its meaning. Finally, I investigate the EU's fight against environmental crime and assess whether this signals a shift from a climate security perspective to an ecological one.

THEORETICAL PERSPECTIVE: FROM CLIMATE SECURITY TO ECOLOGICAL SECURITY

The linkage between environment and security can be drawn in a range of ways. This relationship first came to the forefront of scholarly debates in the early 19th century, when Malthus (1798) expressed concerns about resource scarcity and environmental degradation. In the 1970s and 1980s, the concept of environmental security began to emerge, with works like Ullmann's Redefining Security (1983) arguing for a broader definition of security that included environmental issues. A decade later, Homer Dixon (1991, 1994) focused on the security implications of environmental degradation, examining the conflicts over environmental resources and its impact on conflict. During the same period, the UN introduced the concept of human security in its Human Development Report in 1994 and cited environmental concerns as part of the human security concept.

By the mid-2000s, the link between climate change and security was specifically discussed, with reference to different connotations of security, including human (Matthew, Barnett, McDonald, & O'Brien, 2010) and national security (Campbell, 2008) dimensions. Generally, national and international security discourses have been most prominent, with states as the primary referent objects. However, growing attention has been paid to individuals and communities as referent objects. Notably, the International Panel on Climate Change included a chapter on human security in its 2014 integrated assessment report (Adger et al., 2014).

Conceptually, climate security encompasses both state and human security. In this framework, state security traditionally refers to the ability of states to manage climate-related threats to their sovereignty or power capacities. Human security, on the other hand, focuses on the capacity of individuals and societies to manage sudden and chronic threats like famine, poverty and disease, arising from climate change (Bremberg, 2018). Within the human security approach, the emphasis is placed on human, environmental and social rights (Barnett et al., 2010, p. 18). Therefore, climate security bridges state and human security with climate/environmental phenomena, where people, societies and states have the capacity to prevent and manage climate-related risks. While individual-centered human security emphasizes climate change mitigation, state-centered security approaches focus on adapting the global system to climate change and preserving the status quo.

Although the environmental security perspective emerged early in the 1970s, in 2020, after the COVID-19 pandemic, a focus on dangers of biodiversity loss and habitat disruption on the human security came to the forefront of public debates. From this perspective, Dalby (2022, p. 4) attempted to redefine environmental security, to include both climate change and biodiversity loss as top priorities to tackle. He argued that the linkage between security and environment is not a new topic, however, the debate in the 1970s faded when neoliberal political ambitions took precedence over all other concerns. He claims that power now has to be reinterpreted in ecological terms and focused on the flourishing of adaptable ecological systems rather than physical domination and the imposition of particular modes of conduct on both humans and what is increasingly inaccurately termed “the natural world”. Whereas the environmental security concept deals with environmental degradation and its security implications, the referent objects remain states and human beings. As Dalby highlights (2022, p. 9), “environmental security is an aspirational discourse, aspiring to a future that is a sustainable ecological context for humanity.”

Thus, although environmental concerns such as biodiversity loss and climate change have been included in the redefinition of security, the impact of climate change on future generations and other living beings is often overlooked. Recent literature aims to go beyond the human-state security dichotomy by incorporating ecological rights into the definition of security. McDonald emphasizes that the relationship between climate change and security is complex, with various perspectives to consider. He proposes four security discourses, each addressing different referent objects: people (human security), nation-states (national security), the international community (international security), and ecosystems (ecological security).

McDonald defines ecological security as a discourse “oriented toward ecosystem resilience and with it the rights and needs of the most vulnerable across time, space, and species: impoverished populations in developing states; future generations; and other living beings” (McDonald, 2018, p. 155). Thus, the concept of ecological security shifts the referent object to ecosystems, recognizing the interconnectedness between human communities and the natural world (McDonald, 2023, p. 7). It emphasizes the interdependence between the needs of human populations and other species (Burke et al 2016), with the entire planet as the referent object. Consequently, the defining feature of ecological security is its emphasis on the primacy of the ecosystem. This non-anthropocentric understanding calls for proactive and radical measures to maintain ecosystem function. Ecological security demands an expanded scope of security threats, emphasizing moral responsibilities towards other living beings and future generations.

McDonald highlights the importance of resilience and a long-term perspective in ecological security. Resilience involves building the resilience of ecosystems and being cautious in exploiting the natural environment, while a future-oriented strategy encourages the transition towards low-carbon or carbon-free economies. Ecological security prioritizes developing the adaptive capacities of vulnerable populations and other assets, as well as future generations.

In contrast to environmental security discourse, which addresses the potential risks and threats posed by environmental degradation to human health and political stability and focuses on the security of human populations in the face of environmental challenges, ecological security discourse advocates for comprehensive reforms to protect biodiversity and ecosystems. This holistic approach encompasses the entire planet, broadens the scale of the climate threat, and encourages action to improve living conditions within the ecosystem. McDonald aims to relocate climate security within a broader environmental philosophy framework, shifting attention from the climate system to the resilience of ecosystems. Therefore, the introduction of the ecological security perspective was an attempt to change the referent object and to extend the scope of security to include climate change alongside other components of the ecosystem.

McDonald (2023, p. 41) asks who the appropriate agents of ecological security are and and what level of responsibility they hold for advancing ecological security. He claims that agents can be found at multiple levels from individuals to international organizations. To explore whether the EU, as an international organization, has the capacity and intention to act as an agent of ecological security, I will examine the evolution of the EU's discourse on the linkage between climate change and security.

THE EUROPEAN PERCEPTIONS OF THE CLIMATE CHANGE AND SECURITY NEXUS

International organizations play a crucial role in fostering international cooperation to address climate-related security risks and develop political responses through climate diplomacy. As climate change is a global challenge, mitigation efforts necessitate the participation of international actors. Within this context, climate change has become a key priority for the EU at both regional and international levels (Van Schaik, 2009, p. 7).

Although the European Commission's Global Assessment of environmental policy document listed biodiversity loss as one of the seven most serious environmental problems as early as 1999 (Baker, 2003, p. 24), throughout the 2000s the EU mostly focused on the security implications of climate change. While the 2003 European Security Strategy recognized climate change as a security challenge, the 2008 report by the High Representative and the Commission identified it as a 'threat multiplier', exacerbating existing threats (High Representative for the CFSP, 2008). This new definition spurred a series of initiatives shaping the EU's climate policies. The EU's 2008 'Climate Change and International Security Report' emphasized the Union's contributions as a security actor on climate change (the High Representative and the European Commission, 2008). Additional reports that year highlighted water scarcity and the climate crisis. In 2009, the EU prepared a document for the UN Secretary General's Report on Climate Change and International Security, underscoring the Union's multilateral leadership.

Starting in the 2010s, the EU aimed to redefine the climate-security nexus. In 2018, the EU committed to deepening the link between climate change and security, focusing on development, humanitarian assistance, conflict prevention, and thereby merging human and international security perspectives. The EU Foreign Affairs Council's Conclusions on Climate Diplomacy acknowledged climate change as a direct factor in international security and stability, resulting in a joint commitment to consider climate-security dynamics in relevant policy areas, especially humanitarian action and early conflict prevention. The EU's recent dialogues with developing countries offer a normative human security framework for climate-related threats.

Despite accelerated efforts in the late 2010s to deepen the climate change-security nexus and introduce an ecological perspective, these elements remain largely separate until the COVID-19 pandemic. In the aftermath of the pandemics, the EU reemphasized the implications of environmental degradation for human security. The 2019 Green Deal prompted the EU to develop new policies for ecosystem security. Executive Vice-President for the European Green Deal, Frans Timmermans emphasized resilience and biodiversity, signaling significant progress towards an environmental security perspective. He claimed that "The coronavirus crisis has shown how vulnerable we all are, and how important it is to restore the balance between human activity and nature. Climate change and biodiversity loss are a clear and present danger to humanity (European Commission, 2020a). Therefore, the EU began to be more inclusive in the name of ecological concerns, without giving up its emphasis on human security as its primary concern.

In the following year, the EU supported the Convention on Biological Diversity (CBD) and the adoption of a new post-2020 global biodiversity framework. In 2022, the EU published its biodiversity strategy for 2030, aiming to build resilience against future threats like climate change, food insecurity, and forest fires (European Commission, 2020b). The Strategy set new targets for nature protection and emphasizes the link between climate change and biodiversity loss, without explicitly addressing their impacts on peace and security. The Nature Restoration Law, adopted shortly after, similarly focuses on ecological restoration without explicitly mentioning peace and security implications. While still recognizing the vital role of conservation, this law seeks to prioritize active restoration of species and habitats. It aims to tackle the interconnected challenges of climate change, water management, and biodiversity loss by addressing their shared underlying causes and implementing integrated solutions (*EU Elections: Achievements and Challenges of the European Green Deal.* (n.d).

As Youngs and Lazard put it:

> The EU has not fully integrated ecological security challenges into its understanding of conflict and instability. While the EU does support the fight against biodiversity trafficking, it has not fully integrated how trafficking of natural resources now plays into complex conflict systems that merge across borders and across continents. The most vibrant ecosystems hosting the most diverse biological reserves are located in fragile and conflict-affected contexts; here,

> transnational crime has merged increasingly with conflict dynamics, leading to the protraction of local, national and regional drivers of conflicts and fragility. Biodiversity trafficking is now the fourth most lucrative illicit economy, ranking closely behind drug and human trafficking. Yet this has not served as a driver of new EU policies in this domain. The fight against biodiversity trafficking and other types of natural resources are not pursued as part of a comprehensive notion of ecological security. (Youngs and Lazard, 2023, p. 165)

The publication of the Strategic Compass and the EU Joint Communication to the European Parliament and the Council entitled "A New Outlook on the Climate Security Nexus" on June 28, 2023 marked a turning point, providing a new understanding of the relationship between climate change, environmental degradation, and security for the EU. This document asserted that both climate change and environmental degradation are risk multipliers and proven drivers for instability and conflict. Furthermore, the Compass highlighted the significance of environmental degradation in the competition for natural resources and global health crises (European Union Council, 2022, p. 22-38). With the New Outlook, the EU has redefined the meaning and implications of the climate-security nexus by explicitly citing environmental degradation alongside climate change. The term "climate and security nexus" now encompasses the impacts of both climate change and environmental degradation, including biodiversity loss and pollution, on peace, security and defense. Additionally, the EU acknowledged the interrelationship between environmental degradation and climate change. The document focused on their combined impact, noting that vulnerable populations in distress are at risk of being targeted by organized crime groups, primarily smugglers. Significantly, the report addresses environmental crime, the fourth largest global crime sector, with the potential to accelerate the climate crisis. The Commission concluded that "the security and defence implications of climate change and environmental degradation have thus become more urgent, challenging, and multifaceted" (European Commission, 2023).

Thus, with the publication of the New Outlook, the security implications of environmental degradation, including environmental crime, were accentuated for the first time, further solidifying the link between environmental degradation, climate change, and security. While the primary focus remained on human beings and member states, the resilience of ecosystems began to be acknowledged more explicitly. As the EU's discourse began to shift towards an ecological security perspective, questions arose about the effectiveness of EU-led policies at the policy level. In other words, as an actor of ecological security, what kind of mechanisms does the EU possess to implement this perspective in practice? The next section explores whether the fight against environmental crime can be an effective tool for the EU to implement an ecological security perspective at the policy level.

One of the core concepts of the ecological security discourse is biodiversity. Thus, at the practical level, actors must engage in biodiversity protection in the name of ecological security. In its efforts towards protecting biodiversity, the EU gives primary importance to the prevention of environmental crimes, including wildlife trafficking, through legal mechanisms. Europol defines environmental crime as activities that breach environmental legislation and cause significant harm or risk to the environment, human health, or both. These offenses include improper collection, transport, recovery or disposal of waste; illegal operation of a factory in which a dangerous activity is carried out or in which dangerous substances or preparations are stored; the killing, destruction, possession, or trade of protected wild animal or plant species; and the production, importation, exportation, marketing or use of ozone-depleting substances (EUROPOL, 2024). Environmental crime constitutes a significant barrier to progress in tackling climate change, addressing biodiversity loss, reducing future pandemics, and achieving sustainable development.

Historically, the EU efforts to address climate change and environmental crime have been handled simultaneously. After accepting climate change as a threat multiplier in 2008, the EU adopted Directive 2008/99/EC on the protection of the environment through criminal law on October 24, 2008. Since then the Directive has become the cornerstone of the EU's legal framework for protecting the environment (European Parliament and Council 2008). According to this Directive, Member States are obliged to provide for criminal penalties in their national legislation in respect of serious infringements of provisions of EU law on the protection of the environment.

In the 2020s, the EU decided to revise the Environmental Crime Directive to include new offenses, increasing the number from nine to eighteen (European Council, 2023). The final draft was accepted in December 2023 (European Parliament and Council, 2023). According to the final draft, "qualified infringements" for environmental crimes have been implemented so that tougher penalties can be adopted in Member States. Significantly, with the adoption of the upgraded version of the Directive, environmental crimes are defined through the destruction or substantial damage that is irreversible or long-lasting to an ecosystem. Thus, the main objective is to protect the environment and the referent object now becomes ecosystems *per se*.

Yet, the same Directive underlined the linkage between environmental crimes and organized criminal groups and terrorist organizations. Thus, although the emphasis is on ecosystems, the implications of environmental crime for national security of member states have not been excluded from the Directive. Environmental crime is described as being the fourth most lucrative criminal activity in the world. Accordingly, recent reports underlined the linkage between organized crime groups, terrorism, and environmental crime. From a different perspective, the EU also underlines the significance of environmental crime and its use by organized criminal groups as accelerating factors for the environmental crisis through the unsustainable exploitation of natural resources (EUROJUST, 2021), thus signaling ecosystems as a referent object of security. Marie Toussaint, MEP for Greens, claims that the New Directive is a victory for the environment, emphasizing the referent object of security as ecosystems. Yet, she also claimed that this Directive "will allow for a more effective and better protection of individuals who suffer as a result of such damage" (The Greens EFA in the European Parliament, 2024). At a discursive level, green policy makers do not neglect human security implications of environmental crime and the referent object remains human beings.

The EU's efforts in the fight against environmental crime have not been limited to enforcement of the Directive in member states, but have included taking on the global leadership role in tackling environmental crime. Within this context, the EU reevaluated its foreign policy mechanisms and redesigned its CSDP missions and operations to incorporate the fight against environmental crime. The Civilian CSDP Compact established in November 2018, highlights that civilian CSDP missions should contribute inter alia to the EU's wider response to tackling new security challenges. In 2021, The European Parliament delivered its first report entitled "Preparing the CSDP for the new security environment created by Climate Change". In November 2022, the EEAS officially proposed a mini-concept to support host States in combating environmental crime through civilian CSDP efforts (Sabatino et al., 2023)[4]. Following this, the EULEX CSDP mission actively pursued environmental protection by addressing environmental crimes as legal matters (EULEX, 2019b). This approach effectively elevates environmental protection to a matter of international law enforcement, shaping the EU's foreign policy and global security concerns.

The European Commission adopted a communication on the EU Action Plan against Wildlife Trafficking (European Commission 2022b). Wild animal trafficking, as an environmental crime, has serious consequences for ecosystems as 83% of wild animal biodiversity has disappeared (Schoonover et al., 2021). The action plan reaffirmed the EU's intention to establish stronger measures against wildlife trafficking in the name of biodiversity protection. Like the US Intelligence Threat Assessment Reports, this document highlights the risks of global health issues that biodiversity loss may cause (European Commission, 2022a). The EU accelerated its efforts to build partnerships with the UN in the realm of environmental crimes. To protect species like rhinos, tigers, and pangolins, EU member states contributed to drafting a landmark United Nations General

[4] The European Union Rule of Law Mission in Kosovo (EULEX) was launched in 2008 as the largest civilian mission under the Common Security and Defence Policy of the European Union. EULEX mission supports selected rule of law institutions şn Kosova on their path towards increased effectiveness, sustainability, multi-ethnicity, and accountability, free from political interference and in line with international human rights standards and best European practices.

Assembly (UNGA) resolution on wildlife crime, adopted in September 2017 (Weatherley-Singh, 2018). As this Action Plan demonstrates, the protection of species has a crucial significance for protecting European populations and preventing global pandemics. However, the referent object of the Plan continues to be human security.

In conclusion, while the EU invests considerable effort in implementing an ecological security perspective, ostensibly defending the entire ecosystem, the referent object remains European populations and the member states in which they are living. Thus, for the EU, environmental security discourse remains the central perspective, directing European policies. It can be concluded that the EU's emphasis has largely remained on the security of its member states and European populations, not exclusively changing the referent object of the new security discourse.

CONCLUSION

The EU's journey from a focus on climate security to a broader embrace of ecological security is a complex and evolving one. This shift prioritizes the well-being of the entire planet, moving beyond a narrow focus on national interests and the well-being of human beings. This study concludes that the evolution of the EU security policy demonstrates a gradual but significant shift. While traditional and human security concerns remain central, there is a growing recognition of the intricate connections between environmental degradation, climate change, and security. This broadening perspective, although still evolving, signals a promising trajectory towards a more comprehensive and holistic approach to security in the face of complex global challenges. Thus, a full transition to ecological security necessitates a more comprehensive integration of ecological considerations into the EU's understanding of conflict and instability. To truly embrace ecological security, the EU must shift its focus from protecting member states' interests to prioritizing the well-being of the entire planet. This requires a more comprehensive integration of ecological considerations into its understanding of conflict and instability, as well as willingness to take bold action to protect biodiversity and ecosystems.

As McDonald suggests, ecological security is best viewed as a form of sensibility or orientation rather than a rigid policy program or definitive set of guidelines (McDonald, 2023a: 97). It calls for a fundamental change in how we perceive and interact with the natural world. For the EU, this means recognizing environmental degradation not merely as a threat multiplier, but as a primary security concern in its own right. It means acknowledging that the security of ecosystems is inextricably linked to the security of humans and states.

This paper also contributes to the integration of environmental crime into security studies. The ecological security perspective blurs the lines between internal/external security domains, as well as national and international dimensions. Thus, incorporating law enforcement considerations is a complementary step towards a more holistic approach to European security.

The paper suggests a revision of the definition of ecological security, demonstrating that it is difficult to separate this concept from human security in practice. Although ecological security traditionally prioritizes ecosystems as its primary focus, the relationship between human security and ecological security remains complex and intertwined, requiring further investigation. As illustrated by the case of the EU Directive on Environmental Crime, any attempt to emphasize human security often necessitates a reconsideration of ecological security, or a more comprehensive framework that analyzes both aspects in tandem. Future studies should reconsider the linkage between human and ecological security.

Moreover, future studies could explore potential institutional developments in law enforcement related to ecological security. The EU's LIFE awards, with the Nature Guardians project as a 2024 finalist, highlight promising initiatives. This project aims to improve environmental conservation by enhancing the efficiency and effectiveness of actions against environmental crime. The project intervened by training over 1,500 agents in Spain and beyond, and producing the first Police Investigation Manual for biodiversity crimes.

REFERENCE LIST

Abrahams D., & Carr E. R. (2017). Understanding the Connections Between Climate Change and Conflict: Contributions From Geography and Political Ecology. *Current Climate Change Reports*, 3(4), 233–242. https://doi.org/10.1007/s40641-017-0080-z

Adger, N, Pulhin, J., Barnett, J., Dabelko, G., Hovelsrud, G., Levy, M., & Oswald, U. (2014). 'Human Security'. In IPCC*, Climate Change 2014: Impacts, Adaptation and Vulnerability*, Cambridge: Cambridge University Press.

Baker, S. (2003). Dynamics of European Union Biodiversity Policy: Interactive, Functional and Institutional Logics. *Environmental Politics*, 12(3), p.23-41.

Barnett, J, Matthew, R. A. O'Brien, Karen. (2010). "Global Environmental Change and Human Security." In R. Matthews et al., (Eds). *Global Environmental Change and Human Security,* Cambridge, MA: MIT Press, p. 3-32.

Benjaminsen, T. A. (2022). The risks of Ecological Security. *New Perspectives,* 31(1), 25-30. https://doi.org/10.1177/2336825x221139697

Bremberg, N. (2018). European Regional Organizations and Climate-related Security Risks: EU, OSCE and NATO. *Stockholm International Peace Research Institute 1*, 1-15.

Brown O, Hammill A, Mcleman R. (2007). Climate change as the 'new' security threat: implications for Africa. *International Affairs*, 83(6), 1141–1154

Burke, A. Lee-Koo, K. and McDonald, M. (2016). "An Ethics of Global Security." *Journal of Global Security Studies*, 1(1), 64–79.

Campbell, K. (Ed.). (2008). *Climatic cataclysm*. Washington DC: Brookings Institute.

Dalby, S. (2022). Introduction to Rethinking Environmental Security. In *Rethinking Environmental Security.* Elgar Online. p. 1-12.

EU Elections: Achievements and Challenges of the European Green Deal. (n.d.). Adelphi https://adelphi.de/en/news/eu-elections-achievements-and-challenges-of-the-european-green-deal?s=03

EULEX. (2019b, November 29). EULEX co-hosted a workshop on Countering Environmental Crime [Press Release]. https://www.eulex-kosovo.eu/?page=2,11,1123

EUROJUST (2021). Report on Eurojust's Casework on Environmental Crime. https://www.eurojust.europa.eu/sites/default/files/assets/report_environmental_crime.pdf

European Council (2023). November 16. Press Release: Environmental Crime : Council and European Parliament Reach Provisional agreement on new EU law. https://www.consilium.europa.eu/en/press/press-releases/2023/11/16/environmental-crime-council-and-european-parliament-reach-provisional-agreement-on-new-eu-law/

European Commission. (2020a). Press Release: Reinforcing Europe's Resilience: Halting Biodiversity Loss and Building a Healthy and Sustainable Food System. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_884

European Commission. (2020b). EU Biodiversity Strategy for 2030: Bringing Nature Back into our lives. https://environment.ec.europa/strategy/biodiversity-strategy-2030.en)

European Commission. (2022a). Press Release: Biodiversity : Stronger Measures against Wildlife Trafficking. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6538

European Commission (2022b) Action Plan Against Wildlife Trafficking. CELEX:52022AE5701. Brussels. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6581

European Commission (2023). Joint Communication to the European Parliament and the Council. A New Outlook on the climate and security nexus: Addressing the impact of climate change and environmental degradation on peace, security, and defence. JOIN 2023() 17 FINAL. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX %3A52023JC0019

European Parliament and Council. (2008). Directive 2008/99/EC of the European Parliament and of the Council of 19 November 2008 on the Protection of the environment through criminal law. Official Journal of the European Union. L328, 28-37.

European Parliament and Council. (2023). Proposal for a Directive of the European Parliament and of the Council on the protection of the environment through criminal law. (COM(2021) 804. Final.

European Parliament (2024). https://www.europarl.europa.eu/doceo/document/ENVI-PA-731606_EN.pdf

European Union Council. (2022). A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values, and interests and contributes to international peace and security. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

EUROPOL (2024). Environmental Crime. https://www.europol.europa.eu/crime-areas/environmental-crime#:~:text=Environmental%20crime%20covers%20the%20gamut,%2C%20human%20health%2C%20or%20both.

High Representative for the CFSP (2008). 'Report on the implementation of the European Security Strategy—Providing Security in a Changing World', Brussels.

High Representative and the European Commission to the European Council (2008). Climate Change and International Security. S113/08. https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/99387.pdf

Homer-Dixon, T. (1991). On the Threshold: Environmental Changes as Causes of Acute Conflict, *International Security*, 16(2), 76. https://doi.org/10.2307/2539061

Homer-Dixon, T. (1994). Environmental Scarcities and Violent Conflict: Evidence from Cases, *International Security*, 19(1), 5–40.

Koubi, V. (2019). Climate change and conflict. *Annual Review of Political Science* 22, 343–360.

Lazard, O. & Youngs, R. (2021). The EU and Climate Security : Toward Ecological Diplomacy. *Carnegie Endowment for International Peace*. https://carnegie-production-assets.s3.amazonaws.com/static/files/files__Youngs_and_Lazard_EU_Climate_FIN AL_07.08.21.pdf

Malthus, T. R. (1998). *An Essay on the Principle of Population*. London, Oxford World Classics.

Matthew, R., Barnett, J., McDonald, B., & O'Brien, K. (Eds.). (2010). *Global environmental change and human security*. Cambridge, Mass: MIT Press.

McDonald M. (2018). Climate change and security: towards ecological security? *International Theory,* 10(2), 153-180. doi:10.1017/S1752971918000039

McDonald, M. (2023). *Ecological Security. Climate Change and the Construction of Security.* Cambridge University Press.

Office of the Director of National Intelligence (2023). Annual Threat Assessment of the US Intelligence Community. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

Sabatino, E., Mesarovich, A., Vaisanen, A., Schnitzler, G., Santopinto, F. (2023). Case Studies of the EU's CSDP Activity. *ENGAGE Working Paper Series*. 19.

Schoonover, R., Cavallo, C., Caltabiano, I. (2021). The Security Threat That Binds Us. The Unraveling of Ecological and Natural Security and What the United States Can Do About It? Edited by F. Femia and A. Rezzonico. The Converging Risks Lab. An Institut of the Council on Strategic Risks. Washington D.C.February.

The Greens/EFA in the European Parliament (2024). Press Release: A Victory in the Fight Against Environmental Crime. February 27. https://www.greens-efa.eu/en/article/press/a-victory-in-the-fight-against-environmental-crime

Theisen, O. M., Gleditsch, N. P., & Buhaug, H. (2013). Is climate change a driver of armed conflict?. *Climatic Change* 117(3), 613–625.https://doi.org/10.1007/s10584-012-0649-4

Trombetta, M. J. (2008). Environmental Security and Climate Change: analysing the discourse. *Cambridge Review of International Affairs*, 21(4), 585-602.

Ullman, R. H. (1983). Redefining Security. *International Security*, 8(1), 129-153.

Van Schaik, L. (2009). The Sustainability of the EU's Model for Climate Diplomacy. In S. Oberthür & M. Pallemaerts.*The New Climate Policies of the European Union: International Legislation and Climate Diplomacy*. VUB Press.

Weatherley-Singh, J. (2018). Is the EU doing enough to address wildlife crime? *Climate Diplomacy*. https://climate-diplomacy.org/magazine/environment/eu-doing-enough-address-wildlife-crime

Weston, P. (2024, May 9). Biodiversity loss is the biggest driver of infectious disease outbreaks, says study. *Guardian*. https://www.theguardian.com/environment/article/2024/may/09/biodiversity-loss-is-biggest-driver-of-infectious-disease-outbreaks-says-study

World Economic Forum (2024). The Global Risks Report 2024. https://www.weforum.org/reports/global-risks-report-2024

Youngs, R. & Lazard, O. (2023). "Climate, Ecological, and Energy Security Challenges facing the EU, New and old Dynamics". In T. Rayner, K. Szulecki & S. Oberthür (Eds). *Handbook on European Union Climate Change Policy and Politics*, p. 158-172.

Vladan Borović[1]
Vojkan Nikolić[2]
Stefana Matović[3]

SOFT POWER DIPLOMACY AND COMPUTER SCIENCE

Abstract

Introduction/Aim of the conducted research: Soft power has allowed a number of states to expand their influence and shape the behavior of other countries without the use of military force or economic sanctions. In the era of scientific development and expansion, computer science can be used as a tool to get other countries to adopt policies and rules promoted by diplomacy. Basic assumption of the research: Over the years, the authors have actively participated as members of Soft Power & Cultural Diplomacy Group, Harvard Belfer Center's Future of Diplomacy Project and The Future of Cultural Diplomacy Project, Harvard Kennedy School, Boston, USA. The assumption is: soft power diplomacy shapes other countries' laws and rules. Methods: Readers of this paper will better understand how the power of computing and the arts has repeatedly been deployed by the U.S. and other governments to help achieve foreign policy objectives. The authors of this scientific paper examine the history of soft power diplomacy, the main principles, numerous successful examples from around the world, and a case study, especially focusing on the USA. Results and Conclusion: The main focus is on the use of newly developed computer hardware and software, technologies, algorithms, technical fields like Artificial Intelligence and Neural Networks in the area of influencing on other countries' policies and laws.

Keywords: *Soft Power, Diplomacy, Computer Science, Security.*

INTRODUCTION

By all means, cultural diplomacy is definitely one of the oldest and most important tools of state governance. It is often referred to as soft power, the power of culture offers the ability to create connections and persuade in a way that may advance national interests more effectively than traditional diplomatic and geopolitical means. The soft power of cultural diplomacy offers a country the potential to apply culture to obtain preferred outcomes by attraction rather than coercion (e.g., military might) or

[1] Ministry of Internal Affairs, Serbia, Belgrade, Serbia, vladan.borovic@mup.gov.rs

[2] Criminalistics and Police University, Serbia, Belgrade, Serbia, vojkan.nikolic@kpu.edu.rs

[3] Geographical institute "Jovan Cvijić" SASA, Belgrade, Serbia, s.babovic@gi.sanu.ac.rs

payment (e.g., economic sanctions). In other words, a nation's ability to influence by attraction rather than by promotion. [1]

For a long period of time, cultural diplomacy has taken many different forms. Several cultural dimensions have been used to connect following the idea of building strong bridges and gaining mutual trust. Some of the nation's most powerful tools are its own cultural influence: Bollywood in India, Hollywood in the U.S., the American university system, art history of Europe, Serbia's sports, culture and architecture, Tesla, Japan's culinary traditions, and the nature of Africa. These resources are underappreciated and therefore underutilized far too often.

There are important examples of artists using their work to create bonds across different cultures. Beethoven composed for the diplomats at the Congress of Vienna in 1814 and he not only produced Symphonies 7 and 8 there, but his next work, the Ninth Symphony, celebrated the peace achieved at that event. "Ode to Joy" from the fourth movement became the European Union's anthem. People around the world still celebrate it for its theme of brotherly love.

It is important to mention that the ability of artists to connect deeply at a human level has resulted in many serving as diplomats. There is a long list of poet-diplomats including Ivo Andric, Gabriela Mistral, Pablo Neruda, Czeslaw Milosz and Octavio Paz. The U.S. has worked with artists to promote Franklin Delano Roosevelt's "Good Neighbor Policy." Our country also turned to jazz musicians from Louis Armstrong to Herbie Hancock to connect with the closed societies of Cold War-era Eastern Europe. One cannot forget the impact that pianist Van Cliburn had in connecting the U.S. and the Soviet Union when, in 1958, he won the inaugural Tchaikovsky International Piano Competition in Moscow.

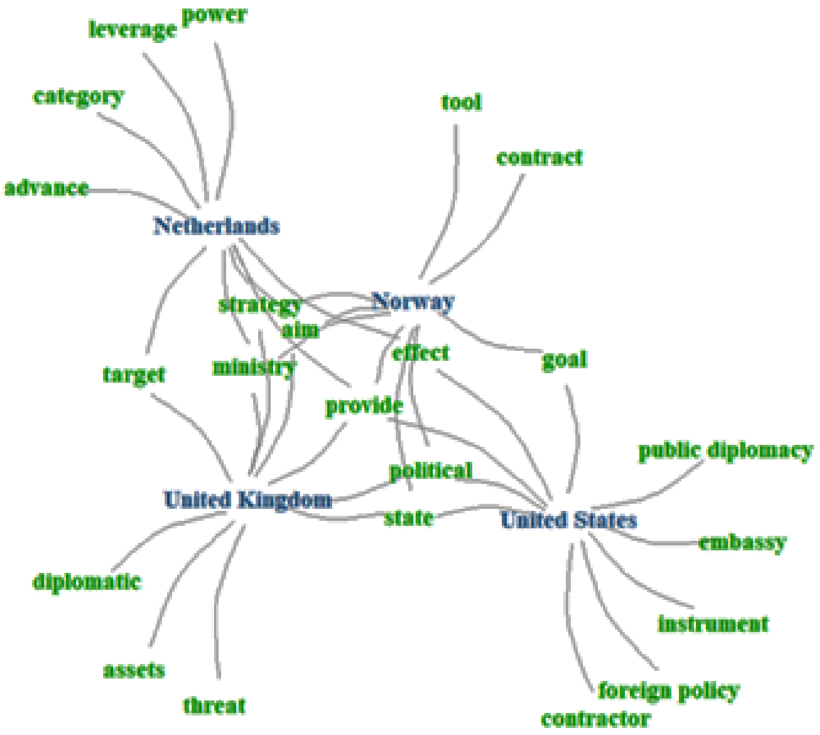
The task of traditional diplomats is to manage relationships with their counterparts in other governments. Though their role is primarily government-to-government engagement, there is an opportunity for much more. Public diplomacy enables governments to reach out and influence entire societies. While some public diplomats communicate with speeches and articles, artists follow another path, connecting with the audiences by touching their hearts. Cultural diplomacy can largely succeed where the best-crafted political negotiations fail.

The best way to learn about the power of cultural diplomacy is to do it.

Some examples include: In Honduras children wrote and performed songs to share their experiences and emotions during COVID-19. A virtual Values Camp was created to help teach kids about integrity, citizenship and entrepreneurship. The goal of this work is for the participants to take pride in their own culture, and to share our mutual appreciation for being good citizens of any country.

We believe cultural diplomacy should be used to further foreign policy objectives. Most effective exchanges have occurred in the People's Republic of China. The real power of listening. We noted their deep appreciation for foreigners who would make an effort to learn their language. This has resulted in growing young audiences for American culture, Hollywood movies, Disney children films and music (hip-hop, rap, techno, rock). At the same time, we in the U.S. and Serbia have become more aware of traditions such as the Chinese New Year.

Figure 1: *Top 10 soft power keywords in four countries*



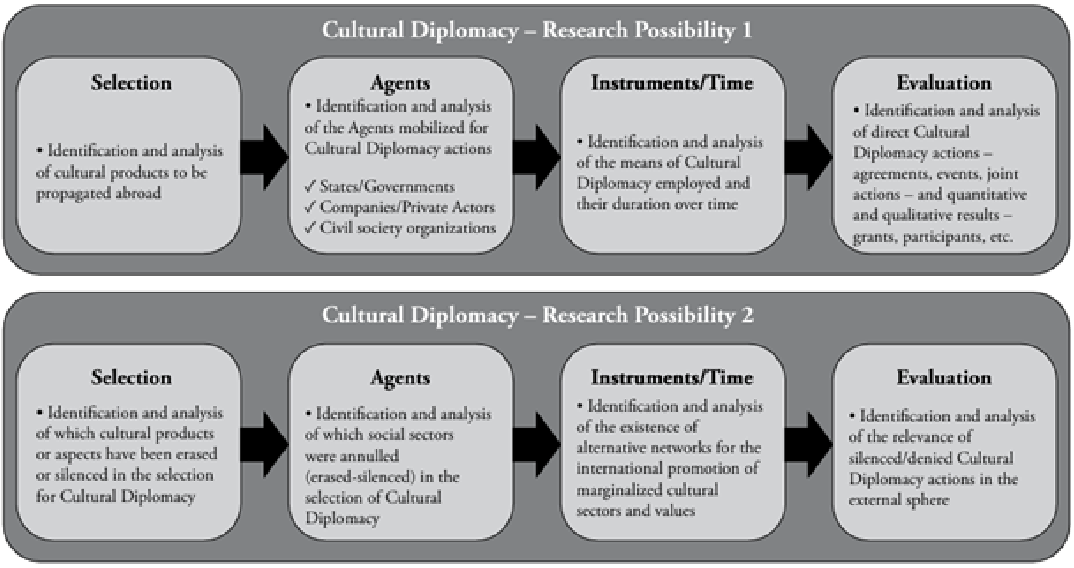
Source: British Council & Schar School of Policy
and Government George Mason University

This was a very important moment for us. Even though we are connected globally more than ever before in history: *Tension arise because of differences in beliefs.*

The solution lies in culture, not just for new diplomatic or national initiatives but for bringing together society into the kind of global community. We can embed culture into diplomacy, we can do more. By harnessing the power of culture, we can achieve great things, starting with a better understanding of each other as people first. Culture reminds us of our common humanity. That sure is a very essential place to start.

The attractiveness of the ideas and positions of the issuing agent should generate adherence by the target audience to a desired behavior without the need for threats.

Figure 2: *Soft power research design possibilities*


Cultural Diplomacy – Research Possibility 1
Selection
• Identification and analysis of cultural products to be propagated abroad
Agents
• Identification and analysis of the Agents mobilized for Cultural Diplomacy actions
✓ States/Governments
✓ Companies/Private Actors
✓ Civil society organizations
Instruments/Time
• Identification and analysis of the means of Cultural Diplomacy employed and their duration over time
Evaluation
• Identification and analysis of direct Cultural Diplomacy actions – agreements, events, joint actions – and quantitative and qualitative results – grants, participants, etc.
Cultural Diplomacy – Research Possibility 2
Selection
• Identification and analysis of which cultural products or aspects have been erased or silenced in the selection for Cultural Diplomacy
Agents
• Identification and analysis of which social sectors were annulled (erased-silenced) in the selection of Cultural Diplomacy
Instruments/Time
• Identification and analysis of the existence of alternative networks for the international promotion of marginalized cultural sectors and values
Evaluation
• Identification and analysis of the relevance of silenced/denied Cultural Diplomacy actions in the external sphere

Source: Cultural Diplomacy and Soft Power: critical analysis and methodological application)

HISTORICAL FACTS

Cultural Diplomacy has existed as a practice for a long period of time, even for centuries. While the term "cultural diplomacy" has only recently been established, evidence of its practice can be seen throughout history and has existed for centuries. Explorers, travelers, traders, teachers, and artists can all be considered living examples of “informal ambassadors” or early “cultural diplomats”. Indeed, any person who interacts with different cultures (currently or in the past), facilitates a form of cultural exchange, which can take place in many fields such as art, sports, literature, music, science, business, economy, and beyond. [2]

Throughout history, the interaction of peoples – the exchange of language, religion, ideas, arts, and societal structures – has consistently improved relations between divergent groups. For example, the establishment of regular trade routes enabled a frequent exchange of information and cultural gifts, and expressions between traders and government representatives. Such deliberate efforts of cultural and communication exchange can be identified as early examples of cultural diplomacy.

No longer relegated to the periphery of the international relations discipline, cultural diplomacy today is a vibrant and innovative academic field of research and has successfully established itself as a stand-alone theory and practice.

– Definition

How do we describe Cultural Diplomacy?

"Cultural Diplomacy may best be described as a course of actions, which are based on and utilize the exchange of ideas, values, traditions and other aspects of culture or identity, whether to strengthen relationships, enhance socio-cultural cooperation, promote national interests and beyond; Cultural diplomacy can be practiced by either the public sector, private sector or civil society." [2]

– Practical importance

Cultural diplomacy in practice (applied cultural diplomacy) is the application and implementation of the theory of cultural diplomacy, including all models that have been practiced throughout history by individuals, communities, states or institutional actors. These models include, for example, diverse cultural exchange programs, international delegations (e.g., American jazz ambassadors), or sports competitions. The examples are uniquely able to affect intercultural and interfaith understanding and promote reconciliation.

– Global importance

In an increasingly globalized, interdependent world – in which the proliferation of mass communication technology ensures we all have greater access to each other than ever before – cultural diplomacy is critical to fostering peace and stability throughout the world. Cultural diplomacy, when learned and applied at all levels, possesses the unique ability to influence the “Global Public Opinion” and ideology of individuals, communities, and nations.

This can accelerate the realization of the 5 important principles below. By accomplishing the first principle, one enables the second, which in turn enables the third, and so on – until the fifth ultimate principle of global peace and stability is achieved.

The main guidelines are:

Figure 3: *Soft diplomacy guidelines*

Respect & Recognition of Cultural Diversity & Heritage
Constant Global Intercultural Dialogue
Justice, Equality & Interdependence to All
The Protection of Global Human Rights
Global Peace & Stability

– In the Public Sector

Two wider approaches to conducting regional and international relations can be distinguished: that of 'hard power' and 'soft power'. The distinguished political scientist

Prof. Joseph S. Nye has made the renowned distinction between the two, describing soft power as "The ability to persuade through culture, values, and ideas, as opposed to 'hard power', which conquers or coerces through military might".

While the so-called hard power approach has historically been a favored policy of governments in conducting international and regional relations, the increasingly interconnected world stage highlights the need for co-operation on a new level. This is where the role of soft power as a form of cultural diplomacy becomes significant. On this basis, cultural diplomacy is not secondary to political or economic diplomacy, but rather functions as an intrinsic and necessary component of it.

– In the Private Sector

As the move towards more socially responsible business practices gains momentum, the ability to understand and embrace the different values and needs of diverse cultures and societies becomes ever more important. There are many reasons why corporations need to be aware of the differences between cultures in their strategic decision-making process and adopt cultural diplomacy models into their agenda:

- In the era of growing social awareness, corporations with culturally sensitive marketing plans and campaigns will enjoy a positive public opinion and a favorable image, and thus perform better financially.
- Companies seeking to expand abroad, will encounter problems unless they conduct research into, and act according to the cultural differences with the host country.
- Companies with a national focus face a related challenge in ensuring that they are aware of and sensitive to national cultural minorities.

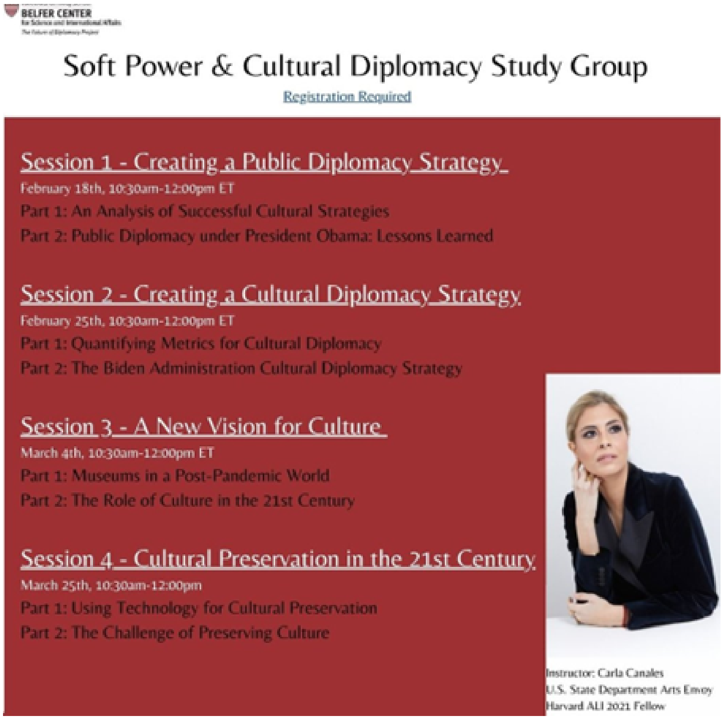
SOFT POWER STUDY GROUP

Over the years, the authors have actively participated as members of the Soft Power & Cultural Diplomacy Group within the Harvard Belfer Center's Future of Diplomacy Project and The Future of Cultural Diplomacy Project at the Harvard Kennedy School, Boston, USA.

More than 100 participants from around the world shared their thoughts, experiences, knowledge, work ethics and cultural facts. In a work and study environment we managed to exchange ideas about the soft power area, share our contacts, and organize online sessions and video workrooms, which enabled us to get to know each other better and gain deeper understanding of our countries' culture and needs.

The Soft Power & Cultural Diplomacy Study Group is designed for anyone interested in learning more about these two topics in addressing foreign relations. Over the course of four sessions, participants will become familiar with the history of cultural diplomacy and will better understand how the power of the arts has repeatedly been deployed by governments to help achieve foreign policy objectives. The group will analyze historical examples and hear from current practitioners. Furthermore, the group will be asked to envision future uses of cultural diplomacy as a tactic for addressing current foreign policy challenges. [3]

Figure 4: *Harvard & US State Department Soft Power Study Group*



BELFER CENTER
for Science and International Affairs
The Future of Diplomacy Project

Soft Power & Cultural Diplomacy Study Group

Registration Required

Session 1 - Creating a Public Diplomacy Strategy
February 18th, 10:30am-12:00pm ET
Part 1: An Analysis of Successful Cultural Strategies
Part 2: Public Diplomacy under President Obama: Lessons Learned

Session 2 - Creating a Cultural Diplomacy Strategy
February 25th, 10:30am-12:00pm ET
Part 1: Quantifying Metrics for Cultural Diplomacy
Part 2: The Biden Administration Cultural Diplomacy Strategy

Session 3 - A New Vision for Culture
March 4th, 10:30am-12:00pm ET
Part 1: Museums in a Post-Pandemic World
Part 2: The Role of Culture in the 21st Century

Session 4 - Cultural Preservation in the 21st Century
March 25th, 10:30am-12:00pm
Part 1: Using Technology for Cultural Preservation
Part 2: The Challenge of Preserving Culture

Instructor: Carla Canales
U.S. State Department Arts Envoy
Harvard ALI 2021 Fellow

Key Benefits

Gain an understanding of cultural diplomacy and its relevance to the government and artistic sector; Learn about important global cultural diplomacy initiatives and analyze their outcomes. Explore the use of cultural diplomacy and soft power as tools to further U.S. foreign policy objectives; Understand public diplomacy and how it differs from cultural diplomacy Assess present-day foreign affairs and national security challenges in a cultural context, and consider how cultural diplomacy and soft power can play a role in seeking resolutions; Discuss why cultural diplomacy is not always successful and what can be done to prevent this from happening.

As shown in Fig. 4. Sessions were:

Session 1 - Creating a Public Diplomacy Strategy
Part I: An Analysis of Successful Cultural Strategies
Part II: Public Diplomacy under President Obama: Lessons Learned
Session 2 - Creating a Cultural Diplomacy Strategy
Part I: Quantifying Metrics for Cultural Diplomacy
Part II: The War in Ukraine
Session 3 - Cultural Preservation in the 21st Century
Part I: Using Technology to Preserve Culture
Part II: The Role of Culture in the 21st Century
Session 4 - A New Vision for Culture
Part I: Museums in a Post Pandemic World
Part II: The U.S. Department of State's Cultural Diplomacy Strategy

AMERICAN GLOBAL TECHNOLOGY COMPANIES AS AN INSTRUMENT OF SOFT POWER – CASE SURVEY

American technology companies that carry out their business globally have been a key instrument of the soft power of the United States of America for decades. They use advanced digital platforms and services to shape the global digital ecosystem, influencing the way individuals consume information, communicate and do business. Some of the largest and most influential global technology companies are: corporations such as Google [4], Facebook [5], Apple [6], Amazon [7] and Microsoft [8]. These companies, in addition to dominating the technology sector on a global level, also serve as an extended arm of American foreign policy, promoting the values and interests of the United States of America at the world level.

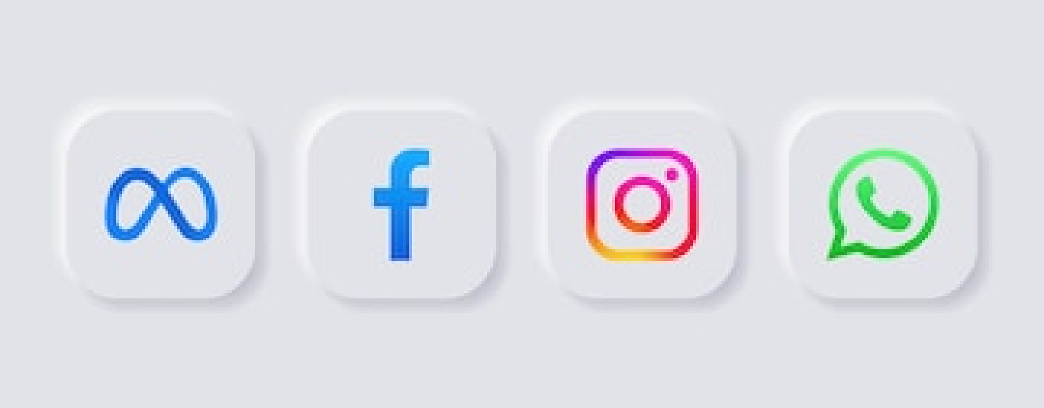
Some of the ways in which American global technology companies strengthen the soft power of the United States are: dominance in digital platforms, promotion of democratic values, and educational and technological influence.

Dominance in digital platforms

American technology companies occupy a dominant position in the global digital ecosystem, influencing the way people search for information, communicate, do business and perform daily activities on the Internet.

The most dominant search engine in the world is a product of Google, with a large percentage share of the global Internet search market. This sophisticated search engine with a complex algorithmic infrastructure provides not only easy access to information, but also shapes the user's perception of the relevance and reliability of certain sources. In addition, its additional solutions, such as Google Maps [9], Google Drive [10] and Google Workspace [11], have become the standard for digital productivity and navigation.

Figure 5: *Digital platforms Meta, Facebook, Instagram and WhatsApp.* [12]



Facebook is the leading platform in the social networking segment. In addition, platforms such as Instagram and WhatsApp [13], Meta [14] and similar have a large share of the social network market. These platforms monitor the communication and interaction of billions of users around the world. They serve not only as tools for social connection, but also as powerful channels for information dissemination, advertising, and political marketing. American dominance in this sector allows the United States to establish the rules of digital communication and create frameworks for the regulation of content, algorithms and business models.

Apple, with its closed ecosystem of hardware and software, also plays a key role in the global digital infrastructure. Its products, such as the iPhone, iPad and MacBook, along with the App Store [15] – a centralized platform for the digital distribution of applications – grant the company complete control over the user experience and access to digital content. Apple's focus on privacy and security further enables it to set the standard for data regulation and cybersecurity.

Amazon dominates both the e-commerce and cloud computing sector. As the world's largest online retail platform, Amazon not only shapes consumer habits, but also sets standards in logistics, shipping and digital advertising. Its AWS (Amazon Web Services) [16] service is a leading provider of cloud solutions, providing infrastructure for companies, governments, and organizations around the world. This level of control gives the United States a strategic advantage in the field of digital services and data storage.

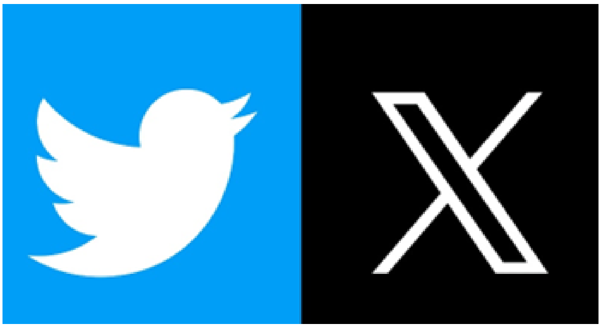
Microsoft, through its Windows operating system, the Office suite, and the Azure cloud platform [17], also has a huge impact on the global digital economy. Its products are the standard in both business and education sectors, while Azure services support many government and corporate IT systems. In addition, Microsoft is investing in artificial intelligence and quantum computing, further strengthening America's dominance in technological innovation.

Thanks to these companies, the United States is not only shaping the future of digital technologies, but also defining regulatory frameworks and security standards. Their dominance allows the United States to dictate the rules of the game in the digital industry, setting the technological, economic and legal standards that other countries must follow if they want to remain globally competitive.

Promotion of democratic values

American technology companies play a key role in the promotion of democratic values around the world, primarily through their digital platforms such as YouTube [18], Twitter (as of 2023 the name has been changed to X) [19] and Facebook. These platforms enable freedom of expression, open access to information and global connectivity, all of which contributes to the development of democracy, civic activism and political participation in different societies.

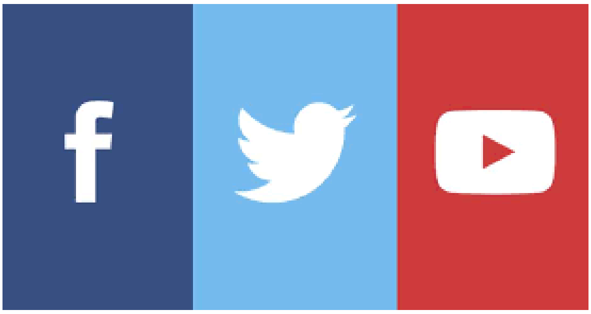
Figure 6: *Twitter (as of 2023 the name has been changed to X).* [20]



One of the most significant contributions of these platforms to democratic processes is their ability to enable the rapid and unhindered dissemination of information. Twitter (renamed X in 2023), for example, has proven to be a key platform for organizing protests and raising awareness of social and political issues. Similarly, YouTube provides a space for investigative journalism and the exposure of corruption through documentaries and citizen testimonies.

Through algorithms that drive content engagement and virality, digital platforms allow important topics to spread quickly and reach a large number of people. This allows marginalized groups and activists to gain a voice and increase the visibility of their demands, even in societies with limited media freedom.

Figure 7: *Digital platforms Facebook, Twitter and YouTube.* [21]



However, the same mechanisms that support freedom of expression can be misused for manipulation and propaganda. Fake news, disinformation and conspiracy theories are often spread on these platforms, which can destabilize democratic institutions and undermine trust in official sources of information.

In addition, algorithmic content selection can lead to the creation of so-called "echo-chamber" (filter bubbles), where users receive information that confirms their existing attitudes, which can contribute to increased polarization of society. Political actors and even foreign governments have used platforms such as Facebook and Twitter (since 2023 the name has been changed to X) for targeted influence campaigns, which is particularly pronounced during election processes.

One of the biggest challenges is content censorship and moderation. While American platforms claim to be committed to free speech, they are simultaneously introducing rules that restrict certain types of content. This is particularly problematic in political contexts, where removing certain posts or terminating accounts can have a significant impact on public discourse and political processes.

Although American technology companies have a significant contribution to make in promoting democratic values through their digital platforms, they also bear responsibility for the negative consequences that arise from their business model. The balance between freedom of expression, regulation of content and prevention of abuse is one of the biggest challenges of the digital era. The future of these platforms will depend on their ability to establish transparent regulatory mechanisms that will simultaneously protect democratic values and prevent their abuse.

Educational and technological impact

American technology companies play a key role in shaping modern education and technology literacy globally. Through innovative digital tools, learning platforms and access to advanced technologies, companies like Google, Microsoft, Amazon, Apple and others are impacting the educational ecosystem, empowering individuals and institutions around the world.

One of the most significant contributions of American companies to education is the creation and distribution of free and accessible educational resources. Google for Education [22] and Microsoft Education [23] offer platforms for learning, collaboration, and the management of teaching processes, using technologies such as artificial intelligence and cloud computing to enhance interactive learning.

Figure 8: *Google for Education and Microsoft Education.* [24, 25]

Google has developed a range of tools, including Google Classroom [26], Google Scholar [27], and digital skills certification programs, while Microsoft provides technology and business professional development through Microsoft Learn and LinkedIn Learning [28]. These platforms help not only students and teachers, but also professionals who want to improve their technical competencies.

In addition to corporate initiatives, US companies are key drivers of global education platforms such as Coursera [29], edX [30] and Khan Academy which offer free and paid courses in a variety of fields, including science, engineering, economics and the arts.

These platforms allow universities like Massachusetts Institute of Technology [31], Stanford University [32] and Harvard University [33] to provide their courses to students from all over the world, reducing the gap in access to education between developed and underdeveloped countries. In this way, the United States strengthens its position as a leader in global education and technological innovation, while simultaneously promoting its values and educational standards.

Along with formal education, US companies also support the development of technological literacy through training programs, certification courses and hackathons. Amazon Web Services (AWS) offers training programs in the field of cloud computing, while IBM [34] and Google provide a wide range of education in artificial intelligence and data analytics through initiatives such as AI for Everyone.

US tech companies are also investing in STEM (Science, Technology, Engineering, and Mathematics) education [35] through partnerships with universities and nonprofits, encouraging young people to get involved in science, technology, engineering and math.

Although these programs bring many benefits, there is concern that the over-dominance of American platforms may lead to cultural homogenization and the imposition of educational standards that do not reflect the specificities of local education systems. Also, the algorithms that govern the availability of courses and resources can create unequal access to knowledge, favoring Western models of education and excluding alternatives from other parts of the world.

Through digital educational platforms and technological innovation, American companies are not only improving access to education but also shaping the future of work and technological literacy. Their influence is undeniable, but it requires constant analysis to ensure that digital education remains inclusive, ethical and adapted to global needs.

CONCLUSION

American tech giants are a key instrument of US soft power, shaping the global digital landscape through dominance in technological innovation, promotion of democratic values, and education. However, their influence comes with significant challenges, including regulatory hurdles, misinformation and geopolitical conflicts. Going forward, maintaining a balance between innovation and accountability will be key to maintaining their dominance in the global digital ecosystem.

As always, the solution lies in culture, not just in new diplomatic or national initiatives but for bringing together society into the kind of global community. We can embed culture into diplomacy, and we can do more. Culture reminds us of our humanity. That sure is a very essential place to start.

REFERENCE LIST

[1] https://www.sir.advancedleadership.harvard.edu/
[2] https://www.culturaldiplomacy.org/index.php?en
[3] https://www.belfercenter.org/publication/soft-power-cultural-diplomacy-study-group-us- department-states-cultural-diplomacy
[4] https://www.google.com
[5] https://www.facebook.com/
[6] https://www.apple.com/
[7] https://www.amazon.com/
[8] https://www.microsoft.com/
[9] https://maps.google.com/maps
[10] https://drive.google.com/drive/my-drive

[11] https://workspace.google.com/

[12] Digital platforms Meta, Facebook, Instagram and WhatsApp

[13] https://www.whatsapp.com/

[14] https://www.meta.com/

[15] https://www.apple.com/app-store/

[16] https://aws.amazon.com/

[17] https://azure.microsoft.com/

[18] https://www.youtube.com/

[19] https://x.com/?lang=en

[20] https://www.tubefilter.com/2023/09/15/x-rebrand-twitter-tweet-survey-report-ad-age-harris-poll-elon-musk/

[21] https://www.netimperative.com/2020/09/24/facebook-youtube-and-twitter-strike-social-media-ad-deal-over-hate-speech/

[22] https://edu.google.com/

[23] https://www.microsoft.com/en-us/education

[24] https://redebeneditina.org.br/google-for-education/

[25] https://www.dict.com.na/product/m365-education-a1/

[26] https://edu.google.com/workspace-for-education/products/classroom/

[27] https://scholar.google.com/

[28]https://www.linkedin.com/learning/

[29] https://www.coursera.org/

[30] https://www.edx.org/

[31] https://www.khanacademy.org/

[32] https://executive.mit.edu/

[33] https://online.stanford.edu/free-courses/

[34] https://www.harvardonline.harvard.edu/

[35] https://www.ibm.com/

[36] https://school-education.ec.europa.eu/en/learn/courses/stem-education#:~:text=STEAM%20Education%20is%20an%20approach,%2C%20dialogue%2C%20and%20critical%20thinking.

Marija Bajagić[1]
Gorica Cvijanović[2]
Boro Krstić[3]

STANDARDS SIGNIFICANT FOR FOOD SAFETY

Abstract

In order to ensure food safety, as well as the consumers themselves, the world food market at the beginning of the 21st century imposed conditions on all participants in the food production chain to have a very responsible attitude towards the quality and healthiness of food. Medical research shows that certain diseases caused by the consumption of unsafe food are on the rise. At the same time, the presence of genetically modified food, which many experts warn against, and whose consequences and influence on the human body will be seen only in a future period, must not be ignored. Food can contain toxic substances of various origins, such as natural toxins, toxic substances created in the process of production, processing and transportation, as well as from the environment. Safe and healthy food is a basic human right guaranteed by the 1948 United Nations Universal Declaration of Human Rights. The legal regulations of almost all developed countries oblige food producers in those countries to introduce standards that define the way food is produced, processed and transported to the consumer in the entire chain of food business "from farm to table". The goal of the standard is to create trust with the customer in terms of the quality and safety of agricultural and other primary products, as well as the reduction of negative impacts on the environment by the current method of agricultural production, the safety of employees in agricultural production and animal breeding. The standards that define food safety are: Global GAP, ISO 22000:2018, HACCP (Hazard Analysis Critical Control Points) with GFSI standard including IFS (International Food Standard), BRC (British Retail Consortium) and FSSC 22000 standard, which will are discussed in detail in this manuscript.

Keywords: *Food Safety, Standards, Healthy Food.*

INTRODUCTION

With the constant growth of food trade at the international level, it is becoming the subject of increasing attention at the universal level, and as such is increasingly becoming

[1] Faculty of Agriculture, University of Bijeljina, Bosnia and Herzegovina, bajagicmarija@yahoo.com

[2] Institute for Science Application in Agriculture, Belgrade, Serbia, cvijagor@yahoo.com

[3] Institute for Science Application in Agriculture, Belgrade, Serbia, direktor@ubn.rs.ba

a global challenge (Negri, 2009) that requires institutional responses. This is particularly evident in the work of the World Trade Organization (WTO) and the Codex Alimentarius Commission. They are the key organizations and institutions that manage food-related risks at the international level. Previous successes in food production are mainly based on the specialization of production, which with the help of modern mechanization, pesticides, mineral fertilizers, newly created varieties of plants, breeds of domestic animals, and huge amounts of energy, achieves very high productivity. This kind of production system is seen as an industrial process in which plants and domestic animals are grown in small factories: the product they produce is larger, with a higher intake of necessary substances, the production efficiency is increased by manipulating their genes, and the soil or water in aquatic systems is only one environment necessary for the growth of plants or farmed animals. In addition, very often such products contain substances that make them unsafe. The quality of food (primary agricultural products) represents a significant basis for the improvement and development of agricultural production as a whole. The weight of that responsibility is increasingly transferred to the producer of agricultural and food products, and quality management systems increasingly represent an important tool for self-control.

Quality is important from the aspect of competitiveness and also has a great influence on the consumer's decision to purchase a product or service. It is one of the most important factors in creating a positive image among consumers for a given product. Quality refers to the chemical composition, physical properties, organoleptic properties, and health status of the product.

From this definition it can be seen that there are 3 types of quality:

- organoleptic properties of the product - refer to appearance, taste, smell, and color;
- commercial product quality - which measures the degree of preparation of each piece of product;
- technological quality - refers to the suitability of the product for processing;

Quality regulations must include the following elements:

- which ingredients the product should contain and its minimum quantities;
- the maximum permitted amount of certain ingredients, as well as certain ingredients that the product can contain;
- which ingredients it must not contain;
- allowed tolerances regarding the amount of individual ingredients;
- ways of storing, keeping, transporting, supporting, and using the product;
- declassification, labeling and labeling of products, packaging and packaging of products;
- conditions and methods of finishing and processing of individual products;
- exemption of certain traffic participants from the application of regulations on quality or certain of its provisions;

According to Rakita (2001), the international organization for standardization emphasizes that "quality is a set of all properties and characteristics of products, processes and services, which refers to the ability to satisfy established or indirectly expressed needs".

FORMAL LEGAL BASIS FOR FOOD SAFETY STANDARDS

In the emerging system of global food safety management, the World Trade Organization plays an important and specific role. Its role stems from the recognized dual effects of food safety standards, where it focuses on their trade effects (Jackson and Jansen 2010). Increasing concern and awareness about food safety directly affect strict regulations (Reardon et al., 2003). At the international level, there are private and public food safety measures. The legislation of developed countries and EU member states is very strict regarding nutrition and the production process. The EU introduced a series of directives, EC 1884/2006, which defines the maximum limit values of toxicants (heavy metals, dioxin, and aflatoxin) that can be allowed in food. Regulation (EC) 396/2005 refers to the highest levels of residues in food of animal and plant origin. Regulation (EC) No. 882/2004kii and Regulation (EC) no. 854/2004 confirm compliance with rules specifically aimed at minimizing risks to acceptable levels and food intake in human food (Roberts & Krissoff, 2004).

In relation to the institutions that form the standard and the certification process, they can be divided into public and private (Table 1).

Table 1. *Division of standards according to their bearers*

Standard	Public	Private
Required	Laws, regulations, rulebooks: e.g., principle of good manufacturing practice; principle of good hygiene practice; HACCP	HACCP
Voluntary	Products with geographical indications, organic production, etc.	ISO, GLOBALG.A.P, BRC, IFS

Source: Mihovski et al., 2012

The basis for the introduction of standards is the Codex Alimentarius (CA), which was established as part of the standards of the World Health Organization with the aim of creating food standards and guidelines. The CA Commission sets standards on food safety and quality, which includes standards for food products and technological or hygienic system codes. Furthermore, it also defines guideline parameters for contaminants and pesticide residues. According to Henson and Humphrey (2009), the

Codex Alimentarius Commission has a significant corresponding position in the development of rules and regulations, so the Codex standards have become current international standards and benchmarks for food safety legislation.

In the context of food safety, the goal is to create common international public standards (Gruszczynski 2006). Increasing concern and awareness about food safety are directly related to strict regulations (Reardon et al., 2003).

During the last few decades, the role of certification worldwide has taken on an exceptional place in terms of meeting the requirements of the international market for food safety and security. Progressive progress in food production plays an important role in the participation of agriculture in the creation of gross social income.

Standards are the language of quality for raw materials, products and processes, work, and organization, etc. (Milić et al., 2017). Standards represent a language in the business world that helps people to understand correctly and more fully in the fields of technology, economics and general development. They are a compromise of "agreements" between producers, trade, and consumers in one country for a certain period of time. That is why it is often said that standards represent order in work and life, because they enable proper communication between workers when solving problems related to quality. The basic meaning of introducing standards into production is:

- rational use of raw materials,
- development of work methods, measurement, evaluation, organization of production,
- increasing productivity,
- quality improvement,
- reduction of production costs,
- faster and more efficient cooperation of one country's economy with other countries, etc.

Standards complement the description of quality much more simply. Standards are elements of quality; however, quality is not always a standard. Often a standard can be composed of several standards. For example, the finished product quality standard consists of:

- the standard that describes the construction,
- standards for terminology,
- standards for dimensions,
- standards for reducing dispersion,
- standards for raw materials,
- standards for features,
- standards for examination and verification.

The basic objectives of standardization were prescribed by the International Organization for Standardization:

1. improving the general economy of human efforts, materials, forces, etc. in the production of products or services;
2. protection of consumer interests through the appropriate quality of goods and services;
3. safety, health and protection of life
4. facilitating the expression and mutual understanding of all interested parties.

The last few decades have seen major climate changes, as well as excessive environmental pollution, which has threatened the entire agricultural sector. Therefore, all producers of food products are at risk. That is why it is very important to monitor the safety of food and products that are placed on the market in order to avoid crisis situations such as food poisoning, loss of clients, etc.

International standards prescribed by the International Organization for Standardization (ISO) define the application and management of quality in all stages of production, processing, and distribution. The quality management systems ISO 9000 and ISO 22000 form the basis of modern production. This also includes food production (Babović, 2005). IFS (International Food Standard) and BRC (British Retail Consortium) are very important in food safety management. These standards can be applied to every processing operation in which food is handled, that is, from the very beginning of production, then the packaging of fresh products, through slaughterhouses, to the processing of food into cans, as well as during the production of highly hygienic products. These standards are accepted by the Global Food Safety Initiative and developed with the aim of verifying the competence of food producers in terms of food safety and quality. The structure of both standards is adapted to the HACCP standard and to Good Manufacturing Practice and Good Hygiene Practice.

The introduction of quality standards in food production is becoming a necessity but also a legal obligation in the Republic of Serbia, so it is necessary to inform and educate producers in primary food production and the food industry about the necessity of food health control and the necessary HACCP quality standards (Veljković et al., 2007).

HACCP SYSTEM

HACCP (Hazard Analysis Critical Control Points) is a system for identifying, evaluating, and controlling hazards of importance to food safety. HACCP is a management system in which food safety is considered through the analysis and control of biological, chemical, and physical hazards (hazards) from incoming raw materials, handling, production, distribution, and consumption of the final product.

The HACCP system consists of two basic components: HA and CCP.

HA represents risk analysis, that is, the identification of hazards in each phase of food production and the assessment of their harm to human health.

CCPs (Critical Control Points) represent production procedures in which a risk to food safety can be prevented or eliminated or its impact can be reduced to an acceptable level. Simply, it is possible to control them.

The basic goal of the HACCP concept is the production of safe food products. Therefore, HACCP does not refer to the quality of the product but to its healthiness. And that method implies the production of health-correct foods by preventive action, not by consequential (inspection) action. The Hazard Analysis Critical Control Point (HACCP) system for food safety is based on the analysis and control of potential biological, microbiological, chemical, and physical threats during the food production process. In the food production process, the HACCP system is adapted to all types of food products and all types of food production and handling to end users. The HACCP system consists of seven principles:

- carrying out a hazard analysis,
- determination of critical control points,
- determination of critical limits,
- determination of requirements,
- determination of corrective measures,
- establishment of procedures for verification,
- establishment and management of effective records and documentation.

In the EU and World Trade Organization markets, the HACCP system became mandatory on January 1, 2006 (Council Directive 93/43/EEC). Simply, the inclusion of food quality and safety standards in the general system of quality control in companies has become a condition for doing business with partners on the international market. The legal regulations of almost all developed countries oblige food producers in those countries to introduce the HACCP system.

The application of HACCP is widespread in developed economies, while in the European Union it is legally binding by the directive of the Council of Europe (Council Directive 93/43/EEC). Although the directive does not apply to countries that are not members of the European Union, this act indirectly has a significant impact on companies that can export their products to the European Union.

Application of the HACCP system is also a legal obligation in Serbia based on the Law on Veterinary Medicine (Official Gazette of RS No. 91/2005) and the Law on Food Safety (Official Gazette of RS No. 41/2009).

For consumers, this means ensuring the supply of healthy food products to the population and reducing the occurrence of food-borne illnesses.

GlobalGAP SYSTEM

The GlobalGAP quality system was created with the aim of introducing a unique standard in primary agricultural production. The standard was originally developed in 1997 by retailers belonging to the Euro-Retailer Product Working Group, called Europe-Gap. It is most represented in the private sector in the world for primary producers. It was developed from good production practices in accordance with consumer requirements related to agricultural production, that is, products that are consumed fresh. In addition to the production process, this standard also includes the processes of harvesting and immediate handling of products after harvesting, up to entering the processing facilities.

GlobalGAP certification is implemented in more than 80 countries of the world and is mandatory in 60% of the European retail network. In essence, this quality standard monitors the correctness of the product "from the field to the table" and is in accordance with the HACCP standard (Veljković et al., 2007; 2010; Štrbac, 2009).

Global GAP is a standard covering the processes that go into production on the farm (eg feed or seedlings), as well as all work activities on the production of the product until the final product leaves the farm. Global GAP is a unique standard that is applicable to all types of primary products for the production of which specialized requirements are being developed, namely, in:

- crop production - fruits and vegetables, flowers and ornamental plants, combined crops, animal feed, green coffee and teas,
- livestock production - cattle and sheep, dairy products, livestock, poultry,
- aquaculture - trout, salmon, carp, catfish, pike...

The basic principles of the Global GAP standard are: limited and controlled use of all types of agrochemicals; hygienic treatment during the production and manipulation of agricultural products; providing instructions and recording all activities while ensuring traceability; uniform rules that enable unbiased verification (confirmation that everything is done correctly); mutual communication and exchange of opinions between producers, traders and users of products; care for the protection of the human environment and sustainable development; responsible treatment of farm employees; concern for the welfare of farm animals.

Obtaining the GlobalGAP certificate confirms safety and control in food production and ensures better competitiveness of companies on the world market by reducing barriers to the international market and creating conditions for obtaining higher profits.

ISO 22000

Considering that the HACCP system is based on the principles of control of healthy and safe food in production, it can hardly be implemented in large production systems or sales chains. For the purposes of successful implementation of this system, it is necessary to include the ISO 9001 standard, which automatically requires a higher financial cost for the company. These shortcomings of the application of the HACCP system and the ISO 9001 standard implied the creation of a new standard - ISO 22000. The basic postulates for the formation of this standard are the principles of the HACCP system, ISO 9001, and the so-called prerequisite programs (PRP) for large companies engaged in the food industry for the production of a safe final food product. Also, ISO 22000 deals with the forecasting and analysis of a large number of external factors and dangers that, on the one hand, can threaten food safety, and on the other hand, can adversely affect production, the economy of companies and employees.[4]

It is important to note that the ISO standard 22000 – food safety management system – is based on:

- The requirements of the HACCP system (Codex Alimentarius)
- Requirements of ISO standard 9001:2015 – quality management system;
- Prerequisite programs (PRPs) – programs to ensure a hygienic working, service and safe environment, both for employees and for the food that is produced.
- ISO/TS 22004 – food safety management system;
- SO/DIS 22005 – traceability in food and the food chain – General principles and guidelines for the design and development of food safety management systems;
- ISO/TS 22003 – requirements for certification bodies.

The ISO 22000 standard is a management system for food safety, harmonized for all organizations around the world, and which determines the requirements that organizations must fulfill in the entire chain of production and food circulation (it is applied to the production and circulation of food for humans, animal feed, and agriculture, suppliers of non-food products and services (equipment and packaging manufacturers), as well as logistics service providers, all with the aim of ensuring a safe product for the end consumer and increasing user satisfaction.[5]

ISO 22000 represents a set of International Standards dealing with food safety management. This is a group of international standards that includes all organizations in the food chain and defines the requirements of the Food Safety Management System, and can be implemented independently or integrally with other quality systems.

[4] https://www.dqsglobal.com/sr-sp/sertifikacija/iso-22000-sertifikacija-bezbednosti-hrane

[5] https://www.eurostandard.rs/iso-22000-sistemi-menadzmenta-bezbednoscu-hrane/

The ISO 22000 family contains a number of standards, each focusing on a different aspect of food safety management.[6]

- ISO 22000: 2005 and ISO 22000: 2018 contain overall guidelines for food safety management.
- ISO 22004: 2014 provides generic advice on the application of ISO 22000
- ISO 22005: 2007 focuses on food and food chain traceability.
- ISO/TS 22002-1: 2009 contains specific requirements for food production.
- ISO/TS 22002-2: 2013 contains specific requirements for the hospitality industry.
- ISO/TS 22002-3: 2011 contains specific requirements for cultivation.
- ISO/TS 22002-4: 2013 contains special requirements for the production - packaging of food.
- ISO/TS 22003: 2013 provides guidelines for auditing and certification bodies.

ISO 22000 was last revised in June 2018. It replaced ISO 22000:2015. The revision introduced a more modern high-level structure (HLS), which facilitates the integration of the ISO 22000 certificate into the existing management system. From June 29, 2021, companies can only be certified according to the latest ISO 22000:2018 standard.[7]

Figire 1. *Appearance of the logo of the main standards*

Source: www.google.rs

BRC STANDARD

The British Retail Consortium (BRC) standard is a technical standard formed by the leading trade association in Great Britain for the needs of all interested companies in order to ensure the safety and quality of food, with the point of the standard refers to the safety in the food processing supply chain, the preparation of primary products/raw materials for the supply of catering establishments, restaurants or processors, while excluding final consumers (BRC, 2017). Additionally, it can be used to evaluate suppliers and to evaluate production sold under private labels.[8]

[6] https://haccp.rs/iso-22000-2005/

[7] https://www.dqsglobal.com/sr-sp/sertifikacija/iso-22000-sertifikacija-bezbednosti-hrane

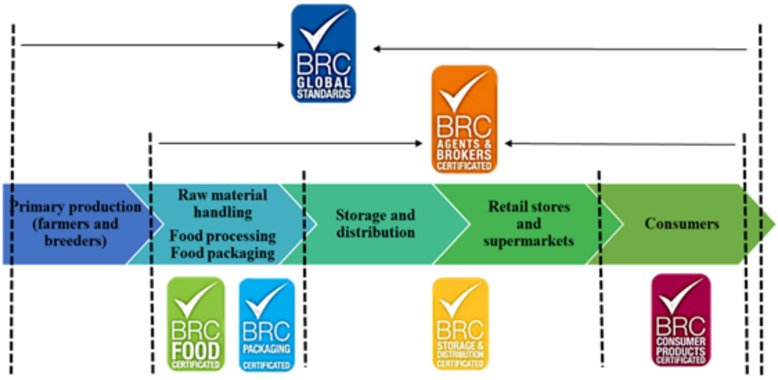
[8] https://www.kvalitet.org.rs/infrastruktura/standardi/brc

The standard operates on integrated compliance with HACCP principles, quality management systems and the application of standards for the control of the factory environment, products, procedures and personnel.

The BRC standard supports the following areas (Figure 2):

- Food safety,
- End products,
- Packaging and packaging,
- Storage and distribution.

Figure 2. *Raspodela standard prema oblastima na koje se odnose:*


BRC GLOBAL STANDARDS
BRC AGENTS & BROKERS CERTIFICATED
Primary production (farmers and breeders)
Raw material handling
Food processing
Food packaging
Storage and distribution
Retail stores and supermarkets
Consumers
BRC FOOD CERTIFICATED
BRC PACKAGING CERTIFICATED
BRC STORAGE & DISTRIBUTION CERTIFICATED
BRC CONSUMER PRODUCTS CERTIFICATED

Source: https://www.kvalitet.org.rs/infrastruktura/standardi/brc

Objectives of the standard[9]:

- Support to users of standards in compliance with legal regulations.
- Prevention, control and protection from health hazards caused by food.
- Greater product safety and lower product liability risks,
- Support in motivating employees and satisfied users.

The principles of BRC standards are[10]:

- Help with accreditation and re-accreditation of obtaining standards
- Support for domestic institutions in assessment and impact on reducing the possibility of double assessment
- Ensuring openness, transparency and compliance with trade laws.
- Suggesting the importance of the participation of retail store owners during the development and maintenance of the system and the committee for technical supervision.
- Control, development and efficiency of the functioning of the standard.

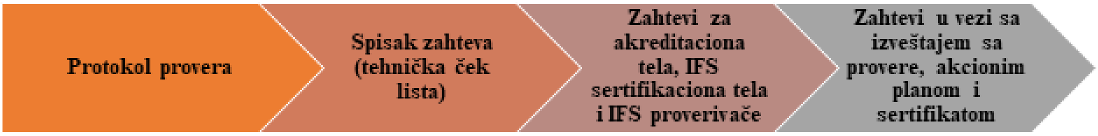
[9] https://www.kvalitet.org.rs/infrastruktura/standardi/brc

[10] https://www.tehnologijahrane.com/enciklopedija/brc-british-retail-consortium-opsti-standard-za-hranu

INTERNATIONAL FOOD STANDARD (IFS)

The International Food Standard (IFS) was formed by a consortium of German, French, and Italian brands to meet the increasing requirements for food quality and safety. The standard is based on the structure of the BRC standard and ISO 9001:2008. The specificity of this standard is that it is comprehensive, as it contains both a quality standard and a food safety standard. The functioning of the standard is based on traceability, i.e. that the quality, safety and correctness of the product follow the products at every moment on the way from the primary producer to the end user at every stage of production and distribution. The standard is applicable throughout the entire food process, except for agricultural production (Figure 3).

Figure 3. *Basic structure of the IFS standard:*


Protokol provera
Spisak zahteva (tehnička ček lista)
Zahtevi za akreditaciona tela, IFS sertifikaciona tela i IFS proverivače
Zahtevi u vezi sa izveštajem sa provere, akcionim planom i sertifikatom

Source: https://www.eurostandard.rs/

Basic objectives[11]:

- Establishing a unique evaluation system
- Accreditation support
- Ensuring safe and transparent product supply
- Help in saving financial inputs and time spent in all processes.

Advantages of implementing IFS standards[12]:

- The possibility of safer and more efficient delivery of safe, good quality food,
- Having a certificate reduces costs at different levels of inspections and checks,
- The certificate enables compliance with legal obligations and regulations,
- Influences the improvement of the popularization of the institution and the brand.

Division of the standard according to purpose (Figure 4)[13]:

- IFS Food - food production;
- IFS Global Markets - Food is a standardized food safety assessment program for retailers, as well as food products in the food industry;
- IFS Wholesale / Cash & Carri - The standard was developed to optimize the

[11] https://haccp.rs/ifs-international-food-standard/

[12] https://www.kvalitet.org.rs/infrastruktura/standardi/ifs

[13] https://www.gsc-standards.com/standardi/ifs.html

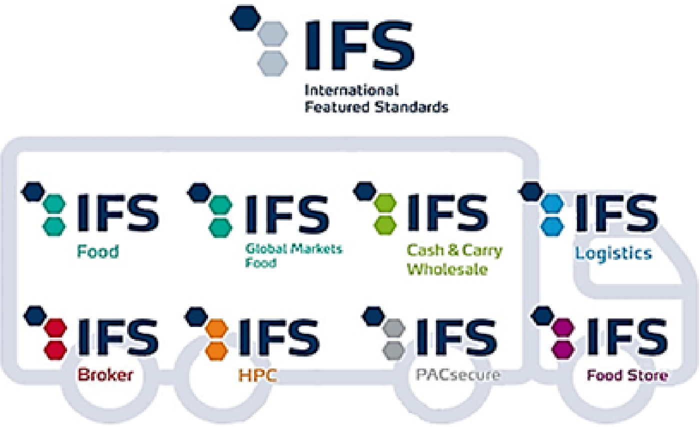
audit procedures of wholesalers and Cash & Carri traders;

• IFS Logistics applies to both food and non-food products and covers all logistics activities, such as loading, unloading and transportation;

• IFS HPC is a standard that ensures product safety, reduces costs and ensures transparency in the entire production chain of household and personal care products;

• IFS PAC secure is a standard for auditing producers of primary and secondary packaging materials.

Figure 4. *Podela IFS standard*



Source: https://asconsulting.rs/ifs-hpc-standard/

According to the basic requirements for food safety and quality, Table 2 shows comparisons of GLOBAL G.A.P/ ISO 22000/BRC/IFS standards.

Table 2. *General requirements of the standard*

	GlobalGAP	ISO 22000	BRC	IFS
Management System	🟡	🟢	🟢	🟢
Hygiene Principles	🟢	🟢	🟢	🟢
Process and Product Control	🟡	🟢	🟢	🟢
Social Responsibility	🟢	🔴	🔴	🔴
Environmental Protection	🟢	🔴	🔴	🔴
Sustainable Agricultural Practices	🟢	🔴	🔴	🔴
🟢 Fully covered request, 🟡 Partially covered request, 🔴 Uncovered request				

Source: Mihovski et al., 2012.

CONCLUSION

The introduction of quality standards enables greater competitiveness in the process of exchanging goods and services, and generally facilitates entering the market of the European Union and beyond, which means that products must comply with the requirements of quality standards such as HACCP and Global GAP. In this way, food safety and quality can be ensured in a simple and traceable way, namely through health, economic, and environmental monitoring through certification and securing the desired certificates.

REFERENCE LIST

Babović, J. (2005): *Agrobiznis u ekološkoj proizvodnji hrane,* monografija, Institut za ratarstvo i povrtarstvo, Novi Sad. (p. 7-36)

British Retail Consortium – BRC. (2017). *Global Standard. Food Safety.* Quick Guide for Issue 7, (available at: https://www.brcglobalstandards.com/media/ 27116/brc-food7-quick-guide-uk-screen.pdf).

Henson, S., & Humphrey, J. (2009). *The impacts of private food safety standards on the food chain and on publicstandard-setting processes*. FAO/WHO Food Standards Programme, Codex Alimentarius Commission, ALINORM 09/32/9D-Part II.

Jackson L. A., Jansen M. (2010). Risk assessment in the international food safety policy arena. Can the multilateral institutions encourage unbsed outomes?", *Food Policy* 35.6, p. 539

Lukasz Gruszczynski (2006). "Science in the process of risk regulation under the WTO agreement on sanitary and phytosanitary measures", *German Law Journal* 7.4, 2006, 372.

Milić D., Lukač Bulatović M. (2017). *Management of fruit and viticulture production,* University of Novi Sad, Faculty of Agriculture.

Mihovski, B., Živadinović, T., Živkov, G., Dulić- Marković, I. & Barjolle, D. (2012). *Guide for certification of agricultural production and food industry*. REDD, SEEDEV & Mena Group.

Rakita, B. (2001). *International Marketing*, Faculty of Economics, Belgrade

Reardon, T., Timmer, C. P., Barrett, C. B., & Berdegué, J. (2003). The rise of supermarkets in Africa, Asia, and Latin America. *American journal of agricultural economics,* 85(5), p. 1140-1146.

Roberts, D. H., & Krissoff, B. (2004). *Regulatory barriers in international horticultural markets: US Department ofAgriculture*, Economic Research Service (PDF) Analysis of Adoption of GlobalGAP Certification in Pakistan. Available from: https://www.researchgate.net/publication/358041067_Analysis_of_Adoption_of_GlobalGAP_Certification_in_Pakistan [accessed Feb 18 2025].

Stefania. N. (2009). Food safety and global health: an inernational law perspective", *Global Health Governance* 3.1, 1.

Strbac, M. (2009): Requirements of the EU market in the field of production and marketing of fruits and vegetables, *Economics of agriculture*, vol. LVI, br. 2 (187-342), pp. 275-282, Belgrade.

Veljković B., Madić M., Bokan, N., Đurić M. (2007): Food quality control and HACCP standards. In: Third international consultation "*Agriculture and local development*", Proceedings, Vrnjačka Banja, Serbia. p. 289-293,

Miranda Gurgenidze[1]
Tamazi Urtmelidze[2]

INTERNATIONAL IP SYSTEMS AND THEIR ROLE IN ADVANCING INNOVATION AND DEVELOPMENT

Abstract

Intellectual property (IP) systems are central to fostering innovation and economic development in a globalized economy. This paper explores the role of international IP frameworks, such as the World Intellectual Property Organization (WIPO) and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), in promoting innovation. The study examines how effective IP protection incentivizes research and development (R&D), technology transfer, and foreign investment while balancing public interest concerns. The research employs a comparative analysis of IP policies in developed and developing economies to highlight best practices and challenges. The findings suggest that while strong IP regimes encourage technological progress, they must be balanced with equitable access to knowledge and fair competition. The expansion of global IP systems, digital transformation, and policy shifts continue to shape the effectiveness of these frameworks in the modern economy. Furthermore, this paper analyzes the roles of the Madrid, Hague, Lisbon, and Patent Cooperation Treaty (PCT) systems in fostering international trademark, industrial design, and patent protection. It highlights their operational structures, advantages, limitations, and future prospects in the evolving landscape of intellectual property law and innovation.

Keywords: *Intellectual Property, WIPO, Madrid System, Hague System, Lisbon System, Patent Cooperation Treaty (PCT), Trademark Protection, Regional IP Systems*

The protection of intellectual property (IP) is a fundamental pillar of modern economies, serving as a catalyst for innovation, technological advancement, and economic competitiveness. In an increasingly interconnected world, where knowledge and creativity drive market growth, robust international IP systems ensure that inventors, businesses, and creators can safeguard their innovations and benefit from their commercial value across multiple jurisdictions. However, navigating the complexities of global IP protection presents significant challenges, particularly due to the territorial nature of IP rights and the varying legal frameworks across different countries. To address these

[1] Faculty of Law and International Relations, Georgian Technical University, Tbilisi, Georgia, gurgenidzemiranda07@gtu.ge

[2] Faculty of Law and International Relations, Georgian Technical University, Tbilisi, Georgia, t.urtmelidze@gtu.ge

challenges, several international treaties and systems have been established under the administration of the World Intellectual Property Organization (WIPO). Among the most significant are the Madrid System for international trademark protection, the Hague System for industrial design registration, the Lisbon System for the protection of appellations of origin, and the Patent Cooperation Treaty (PCT), which simplifies the process of seeking patent protection in multiple countries. These systems aim to harmonize registration procedures, reduce costs, and improve the efficiency of international IP protection while allowing individual nations to maintain sovereignty over their examination and enforcement processes. This paper provides a detailed analysis of these international IP frameworks, exploring their historical development, operational structure, benefits, challenges, role in global brand protection, and future prospects. By examining how these systems contribute to innovation and economic growth, we can assess their effectiveness in fostering a fair and accessible IP landscape. Additionally, the study highlights emerging trends such as digitalization, artificial intelligence (AI), and blockchain-based IP management, which are expected to shape the future of international IP protection. Ultimately, understanding the strengths and limitations of these systems is essential for policymakers, businesses, and legal practitioners striving to create a balanced global IP regime that incentivizes innovation while ensuring equitable access to knowledge and cultural heritage. Development is a multifaceted concept that extends beyond economic growth and modernization. It encompasses social progress, cultural enrichment, human well-being, and environmental sustainability. Historically, economic growth was considered synonymous with development, with many experts identifying GDP expansion and industrialization as primary indicators of progress (Rostow, 1960). However, more recent theories, particularly the capabilities approach introduced by Amartya Sen and Martha Nussbaum argue that true development is about expanding human freedoms and opportunities. Sen emphasizes that economic prosperity alone is insufficient unless individuals can access essential services such as healthcare, education, cultural participation, and a clean environment (Sen, 1999). This shift in perspective has been widely adopted in global development policies, including those of the United Nations Development Programme (UNDP), which integrates human development indices into economic assessments (UNDP, 2019). Intellectual Property (IP), as a legal and economic tool, is deeply interwoven with this broader notion of development, influencing everything from technological innovation to cultural preservation and knowledge dissemination (Maskus, 2000). Development is at the core of WIPO's mandate. When the organization was first established, its role was to promote the protection of intellectual property throughout the world. "Upon becoming a specialized agency of the United Nations in the mid-1970s, this role was more specifically connected to development. Thereafter, WIPO has been tasked to promote creative intellectual activity and technology transfer to developing countries in order to accelerate economic, social and cultural development." Of course, this can be done with flexible systems of intellectual property protection. WIPO promotes development through intellectual property policy in several ways. In addition to being a leading forum for negotiating new treaties and agreements (including their flexibilities).

WIPO:

- administers some of the most important processes for protecting intellectual property rights internationally,
- provides training and education,
- legislative and technical assistance,
- serves as a reservoir of rich databases of intellectual property-related information.

WIPO has, in the past, heard suggestions from its Member States, non-governmental organizations and others to improve work in the area of intellectual property and development. Some of these suggestions date back several decades, since the issue of intellectual property and development surfaced in the 1960s. None, however, have had as much impact as a formal initiative, first advanced by Argentina and Brazil in 2004, for a new and specific ”Development Agenda”. The WIPO Development Agenda sometimes called the ”DA” for short, is part of a change in the ways that links between intellectual property and development are understood, and consequently in the way that development issues are prioritized. For example, this could be by emphasizing flexibilities in the intellectual property system that could help development. As we know, development is no longer viewed as solely about economic growth, and that it is increasingly appreciated how intellectual property alone can or cannot impact development. It must be emphasized again that nothing in the Development Agenda rejects the benefits of intellectual property rights. To the contrary, the Agenda confirms that intellectual property can and does facilitate development in many circumstances. Understanding these circumstances in both local and global contexts will help countries and organizations to better design, administer and use intellectual property systems that the WIPO Development Agenda seeks to further deepen appreciation of this topic. Recognizing both the benefits and costs of intellectual property in light of social, cultural and economic issues actually makes intellectual property a more important subject than if the focus were on protection alone. For example, copyright protection is very important for many kinds of creators, including authors and book publishers. Without copyright protection, it would be much more difficult to set the price and conditions of access to books, which sustains the publishing industry. At the same time, however, copyright protection may not provide the right market incentives to guarantee that books are produced in a manner accessible to everyone, including speakers of local languages or persons with perceptual disabilities. The international copyright system includes a mechanism – an appendix to the Berne Convention –to permit countries to issue compulsory licenses authorizing the translation of books into certain local languages. And negotiations are ongoing among WIPO, its Member States, non-governmental organizations and others about a ground-breaking new agreement for a system to provide the perceptually disabled with access to copyright-protected materials. The WIPO Development Agenda and TRIPS flexibilities demonstrate that IP laws can be tailored to support national development priorities, ensuring a balance between private innovation incentives and public welfare objectives (WIPO, 2007). Moving forward, collaborative policymaking among governments, international organizations, and civil society is essential to create an IP framework that is inclusive, adaptable, and aligned with sustainable development goals (UNDP, 2019).

As nations continue to shape their IP strategies, the emphasis should be on creating systems that promote innovation while also ensuring equitable access to knowledge, healthcare, and cultural resources. Policymakers must recognize that a one-size-fits-all approach to IP does not work – instead, legal frameworks must be responsive to economic, social, and cultural realities (Sen, 1999). Finding the right balance between intellectual property protections and flexibilities like these is key to facilitating access to knowledge and improving people's lives throughout the world. It is an attempt to make the global intellectual property system work better for everyone involved. The WIPO Development Agenda is part of a broader movement reforming and updating the entire international trade framework. It is also important to acknowledge the Doha Development Agenda, named after Doha, Qatar, where the World Trade Organization (WTO) initiated its current round of negotiations. Although these agendas are distinct, cooperation with other organizations, including but not limited to the WTO, on intellectual property (IP)-related matters was one of the key recommendations formally adopted during the 2007 General Assembly of WIPO Member States (WTO, 2001). During this assembly, WIPO Member States agreed on 45 recommendations, categorized into six clusters, which collectively make up the WIPO Development Agenda. The primary objective of these recommendations is to ensure that development considerations are incorporated into all sectors of WIPO's activities. In other words, the aim is to mainstream development across the organization's work. This means that every WIPO initiative should consider the potential economic, social, and cultural impacts of intellectual property (Correa, 2012). Such mainstreaming would be crucial in shaping technical assistance programs, educational initiatives, treaty discussions, and agreements. Additionally, it would serve as a vital evaluation tool for measuring the effectiveness of various intellectual property-related organizations (Gervais, 2008). Following the adoption of these 45 recommendations at WIPO's 2007 General Assembly, considerable effort and discussion were devoted to ensuring their practical implementation. To achieve this, specific activities, programs, and projects were initiated, all of which were overseen by a newly established division within WIPO – the Development Agenda Coordination Division. The DACD functions as the Secretariat for the WIPO Committee on Development and Intellectual Property (CDIP) and plays a central role in coordinating the integration of the Development Agenda across WIPO's operation (Maskus, 2000). Additionally, the DACD acts as the primary liaison with external stakeholders, facilitates discussions on intellectual property and development-related issues, and enhances awareness and understanding of the Development Agenda and its broader benefits (Beall & Kuhn, 2012). Before delving deeper into the six clusters that constitute the WIPO Development Agenda, it is important to highlight that in 2017, the Development Agenda (DA) celebrated its tenth anniversary since its official adoption by WIPO Member States. Over this decade, 35 projects were successfully implemented, providing crucial assistance in various areas of intellectual property while simultaneously ensuring social, economic, and cultural progress (UNDP, 2019). Many of these projects were successfully mainstreamed, meaning that the development dimension became an integral part of several WIPO sectors, thereby fostering sustainable socio-economic growth (Dutfield, 2009). One notable example of a successfully mainstreamed project is the WIPO Technology and Innovation Support Centers (TISC) program. This initiative has evolved into a global program that provides innovators in developing countries, least developed countries, and nations in transition with access to high-quality, locally available technology information and related services (WIPO, 2023h). These resources empower them to maximize their innovative potential, create new inventions, protect their intellectual property rights, and efficiently manage their IP assets (Ginsburg & Janke, 2018).

Global Patent Protection through a Unified System The Patent Cooperation Treaty (PCT), adopted in 1970 and administered by WIPO, is a cornerstone of international patent law that streamlines the process for inventors seeking patent protection in multiple countries. It was designed to simplify, standardize, and reduce the cost of obtaining patents across different jurisdictions by introducing a unified international application system (WIPO, 2023h). Before the PCT, inventors had to file separate applications in each country, leading to redundant administrative processes, legal inconsistencies, and financial burdens. The PCT modernized the patent system by establishing a single application procedure that defers national filings while providing an international search and preliminary examination process (Gervais, 2021d). Since its inception, the PCT has become an essential tool for multinational corporations, research institutions, and independent inventors, supporting global innovation and technological exchange. Operational Structure of the PCT The PCT process is divided into two main phases: the international phase and the national phase. The international phase begins when an applicant files a single international application with a Receiving Office (RO), which is usually the patent office of their home country or WIPO's International Bureau (IB). This application undergoes formal examination, ensuring compliance with basic requirements, before proceeding to an international search conducted by an International Searching Authority (ISA). The ISA issues an International Search Report (ISR) and Written Opinion, assessing prior art and the patentability of the invention. The application is then published internationally after 18 months, allowing public access through the PATENTSCOPE database. Applicants may also request an optional Supplementary International Search, providing broader technical and linguistic coverage of prior art. The International Preliminary Examination (IPE) is another optional step, conducted by an International Preliminary Examining Authority (IPEA). This process allows applicants to amend their claims and receive an International Preliminary Report on Patentability (IPRP Chapter II), which helps them assess the strength of their application before entering national phases (Calboli & de Werra, 2021). The national phase occurs when an applicant proceeds with patent applications in specific countries. At this stage, individual patent offices examine the application under their national laws and either grant or refuse the patent. Each country retains full sovereignty over patent decisions, as the PCT does not provide a global patent but instead facilitates a coordinated international filing process (WIPO, 2023a). Benefits of the PCT System - the PCT significantly reduces complexity and costs associated with filing patents in multiple jurisdictions. By consolidating the application process, it eliminates the need for immediate national filings, allowing applicants to defer costly translation and legal fees until they decide on specific jurisdictions (Gervais, 2021d). The extended 30/31-month timeline enables inventors to assess the commercial potential of their inventions before committing to national-phase filings. Furthermore, the International Search and Preliminary Examination provide applicants with early insights into the patentability of their inventions, helping them refine their claims to improve their chances of approval. Another major advantage is the broad international coverage, as the PCT has 157 contracting states, making it one of the most comprehensive patent systems in the world (WIPO, 2022d). Additionally, the PCT fosters global knowledge-sharing by publishing applications and prior art searches, which helps scientists, researchers, and businesses stay informed about technological advancements and avoid duplication of research (Almeida, & Marques, 2020). Challenges of the PCT System Despite its many benefits, the PCT has limitations. One major drawback is that it does not grant patents – the decision to approve a patent remains with national patent offices, leading to inconsistencies in examination criteria across different jurisdictions (WIPO, 2023). Another challenge is high national phase costs. While the PCT defers expenses, applicants must still pay individual national filing fees, translation costs, and legal representation fees, which can be substantial. Additionally, different countries apply varied patentability standards, meaning an invention approved in one jurisdiction may be rejected in another (Calboli & de Werra, 2021). Furthermore, some countries are not part of the PCT, requiring separate filings in those jurisdictions, adding complexity for global patent seekers. The workload of national patent offices can also impact processing times, as some offices face significant backlogs that delay final patent decisions (Gervais, 2021d). The PCT plays a critical role in protecting innovations and fostering global technology transfer. By offering a unified system for patent filings, it enables companies, universities, and inventors to secure intellectual property rights across multiple jurisdictions. This is especially important in industries such as pharmaceuticals, biotechnology, electronics, and artificial intelligence, where securing patents in multiple markets is crucial for commercial success (Almeida, & Marques, 2020). The PCT also enhances international cooperation by facilitating partnerships between inventors, investors, and companies seeking to license cutting-edge technologies. Moreover, it contributes to economic development by encouraging foreign investment in research and development (R&D) (WIPO, 2023). The widespread adoption of PCT filings signals an innovation-driven economy, attracting businesses to markets with strong IP protections. The PCT is expected to continue evolving with the adoption of artificial intelligence (AI), machine learning, and blockchain technology in patent processing. AI-driven patent searches are improving prior art examination efficiency, while blockchain-based IP registries could enhance the security and transparency of patent records (Gervais, 2021d). Efforts to harmonize national patent laws may also improve the consistency of examination standards, reducing discrepancies between jurisdictions. The expansion of PCT training programs and digital tools aims to increase accessibility for inventors in developing countries, fostering a more inclusive innovation ecosystem (WIPO, 2023c). As global R&D investment continues to grow, the PCT will remain a vital mechanism for protecting inventions, stimulating technological advancements, and supporting economic growth worldwide.

The Madrid System was initially established under the Madrid Agreement (1891) and later modernized by the Madrid Protocol (1989) to increase flexibility for participating countries (WIPO, 2021b). The Madrid Agreement was created to provide a mechanism for international trademark protection, allowing trademark owners to register their marks in multiple countries through a single application (Calboli & de Werra, 2021). However, the system faced several challenges in its early years, including the requirement of a home registration before international filing, which posed barriers for businesses in countries without robust trademark systems (Almeida, & Marques, 2020). To address these limitations, the Madrid Protocol was introduced in 1989, making the system more adaptable. Unlike the Madrid Agreement, the Protocol allows applications based on either registration or pending national applications, expanding access to international trademark protection. The Protocol also introduced flexible renewal deadlines, broader language options (English, French, and Spanish), and extended protection to jurisdictions that had not ratified the original Madrid Agreement. The transition from the Agreement to the Protocol significantly improved the adoption rate, increasing the number of participating countries and making the Madrid System the preferred mechanism for international trademark protection (Gervais, 2021c). Approaches to International Trademark Protection International trademark protection is governed by three primary strategies: national, regional, and international systems. Each approach offers distinct advantages and challenges based on jurisdictional reach, cost-effectiveness, and enforcement mechanisms (WIPO, 2023e). The national system requires businesses to file separate applications in each jurisdiction where they intend to operate. This approach allows countries to maintain control over their trademark laws, ensuring compliance with national commercial interests and consumer protections (Almeida, & Marques, 2020). However, it is costly and time-consuming due to multiple applications and renewal procedures (WIPO, 2022a). The regional system allows businesses to apply for a single trademark registration that covers multiple countries within a specific region (Calboli & de Werra, 2021). These systems are established by treaties among member states and provide a cost-effective alternative to filing separate national applications. Notable regional trademark systems include the European Union Trade Mark (EUTM), the African Regional Intellectual Property Organization (ARIPO), and the Organisation Africaine de la Propriété Intellectuelle (OAPI) (WIPO, 2021). The international system, facilitated by the Madrid System, provides an efficient and flexible approach for businesses to register trademarks in multiple countries through a single international application (Gervais, 2021c). Unlike regional systems, the Madrid System allows applicants to select specific countries from among its 130+ Contracting Parties. As more nations adopt these systems, there is a push towards harmonization and interoperability among the different approaches. The expansion of the Madrid System continues as more countries recognize the need for harmonized international trademark protection (WIPO, 2023e). Several trends are shaping the future of international trademark registration, including digital transformation, AI-assisted trademark search tools, and blockchain-based trademark records that enhance accuracy and reduce duplication in registrations (Gervais, 2021c). Policy reforms within WIPO aim to simplify national registration dependencies and improve procedural transparency for trademark applicants (WIPO, 2022a). Global outreach efforts are underway to encourage non-participating countries, such as South Africa and Argentina, to join the Madrid System, expanding its effectiveness as a truly global trademark mechanism (WIPO, 2023d). With advancements in technology and ongoing trade negotiations, the Madrid System is expected to evolve further, integrating AI-driven automation and smart analytics to enhance the efficiency and security of trademark management worldwide (Almeida, & Marques, 2020).

International Protection of Industrial Designs The Hague System, administered by WIPO, provides a streamlined mechanism for the international registration of industrial designs. It enables applicants to seek design protection in multiple jurisdictions through a single application, reducing administrative complexity and costs. Industrial designs play a vital role in economic competitiveness by ensuring the distinctiveness of products in the marketplace. Protecting industrial designs enhances brand identity and market value, making them an essential component of intellectual property rights (WIPO, 2023a). The Hague System was first established under the Hague Agreement Concerning the International Deposit of Industrial Designs in 1925 to provide a centralized filing system for industrial design protection. Over time, limitations in the original framework led to the development of additional acts, including the London Act (1934) and the Hague Act (1960), which introduced procedural enhancements. The Geneva Act (1999) was the most significant reform, expanding the system's accessibility by allowing applicants from non-member countries to file applications if their home country adhered to the agreement. The Geneva Act also introduced English as an official language, improved fee structures, and allowed for deferred publication of design registrations (Calboli & de Werra, 2021). These developments modernized the Hague System and facilitated its adoption by major economies, significantly increasing its relevance for global industries (WIPO, 2021a). The Hague System operates through a centralized application process administered by WIPO. An applicant files a single international application, which is examined for formal requirements before being transmitted to the designated contracting parties. National or regional IP offices then conduct substantive examinations according to their domestic laws. Unlike patent systems, industrial design applications under the Hague System are not subject to an international search or examination for novelty, meaning that individual jurisdictions retain full discretion over granting protection. The system covers over 90 contracting parties, including key economies such as the European Union, Japan, and the United States. The registration is initially valid for five years and can be renewed up to a maximum term determined by the laws of the designated jurisdictions (WIPO, 2022b). The Hague System simplifies the design registration process by allowing applicants to file one application in one language and pay a single set of fees. This reduces translation, legal, and administrative expenses associated with multiple national filings. It provides flexibility by permitting applicants to designate additional countries at a later stage, accommodating business expansion strategies. The centralized management of design portfolios facilitates easy tracking, renewal, and modification of registrations, improving efficiency for rights holders. Moreover, deferred publication allows applicants to withhold public disclosure for up to 30 months, enabling strategic market entry without premature exposure of design innovations (Gervais, 2021a). Despite its advantages, the Hague System presents several challenges. One significant limitation is that not all countries are contracting parties, necessitating separate national filings in non-member states. Additionally, while the system provides a centralized registration process, each designated jurisdiction applies its own substantive examination criteria, which can result in inconsistencies in the granting of design rights. The lack of an international novelty examination increases the risk of conflicting design registrations. Enforcement remains decentralized, meaning that rights holders must litigate disputes within national courts, leading to jurisdictional complexities and increased costs (Almeida, & Marques, 2020). Furthermore, differences in national laws regarding design infringement and protection scope create additional uncertainties for businesses operating in multiple jurisdictions (WIPO, 2023f). Role in Global Brand Protection Industrial designs contribute to brand differentiation, consumer recognition, and market positioning. The Hague System enhances global brand protection by enabling companies to secure design rights efficiently across multiple markets. This is particularly beneficial for industries such as fashion, consumer electronics, automotive, and luxury goods, where design innovation significantly influences consumer preferences. The system also supports design-driven businesses in protecting their creative assets from unauthorized imitation, reinforcing their competitive advantage. As industrial design infringement becomes increasingly prevalent in international trade, the Hague System provides a critical tool for companies seeking to enforce their rights in multiple jurisdictions (Calboli & de Werra, 2021). The Hague System continues to evolve, with efforts focused on expanding membership and enhancing procedural efficiency. Digitalization is playing a key role in streamlining international design filings, with WIPO implementing AI-powered tools to facilitate design searches and classification. The integration of blockchain technology is being explored to enhance design record transparency and security. Policy discussions within WIPO and participating countries are also considering further harmonization of national substantive examination procedures to reduce inconsistencies in design protection across jurisdictions (Gervais, 2021a). As industrial design protection gains prominence in the global innovation economy, the Hague System is expected to become an even more integral component of international IP strategy, fostering greater accessibility and legal certainty for rights holders worldwide (WIPO, 2023a).

Protection and International Registration of Appellations of Origin - The Lisbon System, administered by WIPO, provides an international framework for the protection and registration of appellations of origin (AO) and geographical indications (GI). It ensures that products linked to specific regions maintain their authenticity, reputation, and economic value in global markets. The system is crucial for industries such as wine, spirits, agricultural products, and handicrafts, where quality and reputation are tied to geographical origin. By granting legal recognition to such products, the Lisbon System strengthens consumer trust and market differentiation, preventing unfair competition and misappropriation (WIPO, 2023b). The Lisbon System was established in 1958 under the Lisbon Agreement for the Protection of Appellations of Origin and their International Registration. The agreement provided a mechanism for securing AO protection through a single registration recognized by all contracting parties. However, its limited membership and rigid requirements restricted broader international adoption. To address these limitations, the Geneva Act of the Lisbon Agreement was adopted in 2015, modernizing the system to accommodate geographical indications alongside appellations of origin. The Geneva Act introduced greater flexibility in national implementation, enhanced procedural efficiency, and expanded accessibility to intergovernmental organizations such as the European Union. This reform strengthened the system's effectiveness and increased its attractiveness to a wider range of countries (Calboli & de Werra, 2021). The Lisbon System allows producers to obtain international protection for their appellations of origin through a centralized registration process administered by WIPO. Applications are filed by a competent authority on behalf of producers, ensuring that only qualifying products receive protection. Once registered, the appellation of origin is recognized across all contracting parties, subject to national laws. Unlike trademarks, which are owned by specific entities, AOs and GIs are collectively managed by producers from the designated geographical region. The Geneva Act introduced procedural enhancements, including the ability to oppose registrations, extend protection to additional products, and allow electronic filing for streamlined processing (WIPO, 2022c). The Lisbon System provides global recognition for appellations of origin and geographical indications, reinforcing product authenticity and consumer confidence. It simplifies the registration process by offering a single application for multiple jurisdictions, reducing administrative costs and legal complexity. The system supports rural and regional economies by enhancing the market value of locally produced goods, fostering economic sustainability. It also prevents the unauthorized use of regional names, ensuring that only genuine producers can benefit from the reputation associated with specific geographic locations. Moreover, international recognition of AOs and GIs facilitates trade negotiations and access to premium markets (Gervais, 2021b). Although the Lisbon System offers various advantages, it faces several challenges. Limited membership remains a significant issue, as many countries have not yet joined the system, requiring producers to seek separate national or regional registrations. Differences in national legal frameworks can create inconsistencies in how appellations of origin are enforced across jurisdictions. Some countries prioritize trademark-based GI protection over AO-based systems, leading to conflicts between national and international approaches. Additionally, proving a strong geographical link between the product and its region of origin can be complex, requiring extensive documentation and evidence. The costs associated with maintaining appellation protection, including enforcement actions against infringers, can also be a burden for small-scale producers (Almeida, & Marques, 2020). The Lisbon System plays a crucial role in global brand protection by ensuring that appellations of origin and geographical indications maintain their integrity. This protection is particularly valuable in industries where regional authenticity enhances product value, such as wine, cheese, coffee, and textiles. The system helps prevent misleading branding practices that could undermine consumer trust and economic benefits for authentic producers. As counterfeit products and mislabeling increase in global trade, the Lisbon System provides a robust legal framework for enforcing rights across multiple jurisdictions. Strengthened international recognition of AOs and GIs promotes fair competition and enhances the competitiveness of local industries in global markets(Calboli & de Werra, 2021).

So, The Lisbon System is expected to expand as more countries recognize the value of protecting appellations of origin and geographical indications. Digitalization efforts within WIPO are streamlining the registration and enforcement processes, making the system more accessible. The integration of AI-based monitoring tools is improving the detection of unauthorized use, strengthening enforcement mechanisms. Ongoing policy discussions aim to harmonize national and international GI protection frameworks, reducing conflicts between different legal traditions. With increasing consumer demand for authenticity and sustainable production practices, the Lisbon System is likely to become a cornerstone of international trade agreements, reinforcing the protection of cultural and economic heritage worldwide (WIPO, 2023g).

As the world continues to evolve into a knowledge-based economy, the importance of strong, yet adaptable, international intellectual property (IP) systems cannot be overstated. The Madrid, Hague, and Lisbon Systems, along with the Patent Cooperation Treaty (PCT), serve as essential tools in ensuring that businesses, innovators, and creative industries have the necessary protections to thrive in an increasingly competitive global marketplace. These frameworks enable the efficient registration and enforcement of IP rights across multiple jurisdictions, offering cost savings, legal certainty, and simplified administrative processes. However, despite their many benefits, these systems are not without challenges. One of the primary obstacles is the fragmentation of national laws that govern IP enforcement. While the PCT, Madrid, Hague, and Lisbon Systems streamline the application and registration process, they do not guarantee uniform protection across jurisdictions. Differences in patentability criteria, trademark laws, and design protection standards can lead to inconsistencies, legal disputes, and barriers to market entry. Additionally, the high costs associated with national phase entries under the PCT, the limited membership of some systems, and bureaucratic inefficiencies in certain jurisdictions remain significant hurdles for businesses and individual inventors. These disparities call for continued efforts to harmonize international legal frameworks while maintaining the flexibility necessary for local adaptation. Furthermore, the rapid advancement of emerging technologies such as artificial intelligence (AI), blockchain, and big data analytics presents new opportunities and challenges for global IP governance. AI-driven patent search and examination processes, blockchain-enabled IP registries, and automated trademark monitoring could revolutionize how intellectual property is managed and enforced. However, these technologies also introduce complexities regarding data security, ownership rights, and ethical concerns, which must be addressed through robust regulatory frameworks and international cooperation. The role of WIPO in coordinating and improving these systems is crucial. While WIPO has made significant strides in facilitating international IP protection, further policy reforms are needed to ensure accessibility, fairness, and transparency in the system. Governments and international organizations must work together to expand participation in existing frameworks, particularly in developing countries where access to IP protections remains limited. Capacity-building programs, financial assistance for small and medium-sized enterprises (SMEs), and knowledge-sharing initiatives should be prioritized to create a more inclusive global IP system. Ultimately, the future of intellectual property protection lies in striking a balance between innovation incentives and public interest considerations. As global markets continue to expand and digital transformation accelerates, policymakers must ensure that IP laws remain flexible, equitable, and responsive to the changing needs of businesses, creators, and consumers. Strengthening international cooperation, fostering innovation-friendly legal frameworks, and leveraging digital advancements will be essential in shaping a more efficient and effective global IP system. In conclusion, while international IP systems have made significant progress in streamlining protections for trademarks, industrial designs, patents, and appellations of origin, there remains much work to be done. By embracing innovation, promoting legal harmonization, and enhancing accessibility, the global community can ensure that intellectual property continues to serve as a driver of economic growth, technological progress, and cultural preservation in the 21st century.

REFERENCE LIST

Almeida, P., Marques, J. (2020). The global impact of the Hague system on design protection. *Journal of Intellectual Property Law*, 26(1), 98-120.

Beall, R., Kuhn, R. (2012). *Trends in compulsory licensing of pharmaceuticals since the Doha Declaration*. PLOS Medicine.

Calboli, I., de Werra, J. (2021). *The Cambridge handbook of international and comparative design law*. Cambridge University Press.

Correa, C. (2012). *Intellectual property and public health: Balancing competing interests.* Edward Elgar Publishing.

Dutfield, G. (2009). *Intellectual property rights and the life science industries: A twentieth-century history.* Ashgate.

Gervais, D. (2008). *The TRIPS agreement: Drafting history and analysis*. Sweet & Maxwell.

Gervais, D. (2021a). The future of the Hague system: Challenges and opportunities. *World Design Protection Review*, 35(3).

Gervais, D. (2021b). The future of the Lisbon system: Challenges and opportunities. *World Geographical Indications Review*, 36(2).

Gervais, D. (2021c). The future of the Madrid system: Challenges and opportunities. *World Trademark Review*, 34(4.

Gervais, D. (2021d). The future of the PCT: Challenges and opportunities. *World Patent Review*, 39(1).

Ginsburg, J., & Janke, T. (2018). *Indigenous knowledge and intellectual property law: Genetic resources, traditional knowledge, and folk expressions*. Cambridge University Press.

Maskus, K. (2000). *Intellectual property rights in the global economy*. Peterson Institute for International Economics.

Rostow, W. (1960). *The stages of economic growth: A non-communist manifesto.* Cambridge University Press.

Sen, A. (1999). *Development as freedom*. Oxford University Press.

United Nations Development Programme (UNDP). (2019). *Human development report 2019: Beyond income, beyond averages, beyond today*. UNDP. https://hdr.undp.org/

World Intellectual Property Organization (WIPO). (2007). *The WIPO development agenda*. World Intellectual Property Organization.

World Intellectual Property Organization (WIPO). (2021a). T*he Geneva Act of the Hague Agreement: A guide for users.* https://www.wipo.int/hague/en/guide

World Intellectual Property Organization (WIPO). (2021b). *The Madrid Protocol: A guide for users*. https://www.wipo.int/madrid/en/guide

World Intellectual Property Organization (WIPO). (2022a). *Madrid system for the international registration of marks*. https://www.wipo.int/madrid

World Intellectual Property Organization (WIPO). (2022b). *The Hague system for the international registration of industrial design*s. https://www.wipo.int/hague

World Intellectual Property Organization (WIPO). (2022c). *The Lisbon system for the international registration of appellations of origin*. https://www.wipo.int/lisbon

World Intellectual Property Organization (WIPO). (2022d). *The Patent Cooperation Treaty and international patent protection*. https://www.wipo.int/pct

World Intellectual Property Organization (WIPO). (2023a). *About the Hague system*. https://www.wipo.int

World Intellectual Property Organization (WIPO). (2023b). *About the Lisbon system*. https://www.wipo.int

World Intellectual Property Organization (WIPO). (2023c). *About the PCT system*. https://www.wipo.int

World Intellectual Property Organization (WIPO). (2023d). *About WIPO*. https://www.wipo.int

World Intellectual Property Organization (WIPO). (2023e). *Madrid system benefits and challenges*. https://www.wipo.int/madrid/en/overview

World Intellectual Property Organization (WIPO). (2023f). The Hague system and global design protection. https://www.wipo.int/hague/en/overview

World Intellectual Property Organization (WIPO). (2023g). T*he Lisbon system and global geographical indication protection*. https://www.wipo.int/lisbon/en/overview

World Intellectual Property Organization (WIPO). (2023h). *WIPO technology and innovation support centers (TISC)*. https://www.wipo.int

World Trade Organization (WTO). (2001). *Doha Declaration on TRIPS and public health*. World Trade Organization.

Emilia Alaverdov[3]

MUNICH SPEECH AND THE BEGINNING OF A 'NEW COLD WAR'

Abstract

Introduction and Aim: The victory in the Cold War made the United States the world's leading power, but the reality soon changed. Globalization made the world even more complex, and this reality required fundamental changes in American foreign policy priorities. Here we have to say that the foreign policy of any state refers to one of the most difficult spheres of its activity. At the same time, the effectiveness of foreign policy depends to a decisive degree on its realism, purposefulness, and consistency. All these characteristics are largely laid down already at the stage of developing projects of relevant doctrines, strategies, concepts, etc. The status of the Russian Federation as the successor state of the USSR was officially recognized by the international community as a whole and by each state individually. All CIS countries recognized this beginning with the decision of the Council of Heads of State on December 21, 1991, when they solemnly asked Russia to continue the USSR's membership in the UN, including permanent membership in the Security Council, and other international organizations. An intensive search for a new foreign policy concept for Russia began. Therefore, the paper aims to highlight key points of the new world order after the end of the Cold War. Methods: The paper is based on certain political documents, reports, analyses, books, and experts' observations. As for the theoretical frame, it applies to the Liberal Empire Theory, formed in 2003 by Anatoly Chubais, and Putin's Doctrine about the Russian-Speaking Population and the Use of Military Force in Post-Soviet Space. Results and Conclusion: Russia became stronger after Vladimir Putin came to power, and it was necessary for the United States to form a new type of relationship. However, the president of Russia considers the country so strong that he started to threaten the world leaders at the 43rd Munich Security Conference, accusing them of undermining global security. Thus, one can claim that these accusations and threats, called the "Munich Speech," led to the foundations for the beginning of a "new Cold War."

Keywords: *Russia, Security, Foreign Policy, War, International Relations.*

[3] Georgian Technical University, Tbilisi, Georgia, alaverdoviemilia07@gtu.ge

DISCUSSION

It is known that the end of the Cold War has been declared many times. For example, it was discussed during the warming of Soviet-American relations in the 1950s and 1970s. The euphoria was short-lived: tensions between the powers arose again. Then, in December 1989, M.S. Gorbachev announced its end after the Soviet-American meeting in Malta, when, as he believed, a real breakthrough in bilateral relations had occurred. However, many did not agree with this. They started talking about the end of the Cold War in 1991, when the Soviet Union ceased to exist (Kennet, 2024). Subsequently, the topic of the end of the Cold War was raised more than once. In particular, in May 2002, the signing of the Moscow Treaty was described as the "final burial of the Cold War." In particular, the parties agreed to "reduce the levels of their strategic nuclear warheads to 1,700-2,200 units," but failed to reach a compromise on what constitutes a "strategic nuclear warhead," and consequently on the methodology for counting warheads. It should be noted that the text of the START I treaty uses a different definition - "strategic warhead" (Armscontrol.ru, 2003).

The Cold War had come to an end, fortunately not only for both countries but for the world as a whole. There was no winner in this war, and its outcome was a strengthening of the security of both the USSR and the USA (Tripathi, 2024). The subsequent collapse of the Soviet Union was the result of the tense situation within the country, and not the efforts of external enemies. George H.W. Bush strongly supported Gorbachev's proposal to conclude a new Union Treaty, which would voluntarily unite the twelve union republics into a federation. Since the United States had never recognized the legitimacy of the forced annexation of Estonia, Latvia, and Lithuania to the Soviet Union, it supported their desire to restore independence. Their independence was recognized by one of its last resolutions by the Soviet parliament elected as a result of perestroika. It was the elected President of the RSFSR, Boris Yeltsin, who conspired with the leaders of Belarus and Ukraine, and together they rejected Gorbachev's proposal to conclude a Union Treaty and created the ineffective Commonwealth of Independent States. This did not happen under pressure from the West or because of the machinations of external enemies, but was an indirect result of the unsuccessful coup attempt in August 1991, when those who bore direct responsibility for the security of the Soviet Union tried to replace perestroika with repression. The coup attempt failed, but it significantly undermined the authority of the Soviet government.

For the United States, the Cold War ended with global dominance. Something like this had probably not happened since the Roman Empire. There was something positive about Pax Americana: for a little over twenty years, the major powers had no conflict with each other. But this could not last forever, because the entire world was changing rapidly and in major ways. Later conflicts between the great powers have resumed, perhaps becoming even more dangerous than during the Cold War.

The meaning of the peaceful end of the "Cold War" is that the great powers voluntarily freed the sphere of international relations from the deposits of malice, suspicion, and mistrust. Not completely, of course, because the inertia of the conflict component, like human society in general and in international relations in particular, is too strong. It would probably be premature to talk about the beginning of a "new era", but still, what happened, happened: the danger of a nuclear war and mutual destruction of the countries of European culture was eliminated by themselves, although the scenario of their self-destruction had every chance of success (Kennet, 2024). After all, the cultural Europeans brought their countries almost to complete collapse in the 20th century during the two World Wars (Vogt, 2024).

The standard of living of Russians in the 1990s did not just decline, it fell catastrophically. But at that moment, in early 1992, when liberal reformers led by the president began "shock therapy", this populist promise provided Yeltsin with a sufficient resource of support. Before each crisis or election, Yeltsin generously distributed promises to the population, declared his readiness to improve matters in this or that sector of the economy. For example, on the eve of the presidential elections of 1996, a whole series of successful populist steps were carried out, including the beginning of a partial payment of the multi-billion-dollar debt to the population for pensions, benefits, and wages. Yeltsin's populist style of speeches and interviews was characterized by the absence of any specific analysis of the problems facing the country (Glinski & Reddaway, 1998).

Almost simultaneously with the decline of the USSR, the process of European integration entered a qualitatively new phase. The Maastricht Treaty on the establishment of the European Union, signed on February 7, 1992, increased attention to solving primarily intra-European problems related to the creation and strengthening of common institutions and the “pulling up” of less developed countries to the standards of leading states (Laursen & Vanhoonacker, 2019). The disappearance of the “Soviet threat” and the emergence of a weakened Russian state objectively reduced interest in it. Among the "unresolved" problems was the withdrawal of troops from Germany, Poland, and the Baltic countries, but this was already a matter of time. The general European mood was noticeably influenced by the former socialist countries and their negative experiences from being in the Soviet bloc. They saw guarantees for preserving their sovereignty in "reunification with Europe", primarily through entry into its security structures. Particularly harsh assessments of the past of not only the USSR, but also the Russian Empire, were heard from this political environment. It was here that the topic of a possible return of a threat from the East in the event of the revival of a strong Russian state was peddled. After the collapse of the bipolar system, the emphasis shifted to the civilizational unity of Europe, which included the countries of Western Christianity. According to this position, they bordered on territories whose peoples professed Islam and Orthodox Christianity and belonged to another civilizational community, not European. It included Russia, the development of which, according to this understanding, was based on a cultural foundation opposite to Europe (Sabry, 2024).

Not only the readiness to integrate into military and economic structures, but also a commitment to democracy and European values were put forward as important factors and conditions for joining the renewed Europe. The issues of democracy and human rights gradually turned into one of the instruments of the European Union's foreign policy concerning the countries of the post-Soviet space that were outside its borders but wanted to bring them closer together. At the same time, great flexibility was revealed in the use of "human rights" issues depending on geopolitical, cultural, and civilizational preferences and other circumstances.

It is obvious that in the post-Soviet direction, the US saw as its main goals the strengthening of security (its own and that of its allies) and, with the weakening of the former geopolitical adversary, its assertion of the role of the sole global leader. Their implementation was linked to the solution of many tasks concerning a weakened Russia. In the area of security, this was the reduction of weapons of mass destruction, primarily nuclear weapons, therefore, the emphasis was placed on disarmament issues in bilateral relations. Strengthening security was conceived in the context of a reassessment of NATO issues, which began during the process of German unification and was actualized by the foreign policy reorientation to the West of Eastern European states that were formally part of the Warsaw Pact, which was already fading in 1990–1991 (De Castro, 2024). In this regard, we have to say that Russian leaders expressed their readiness to join NATO in various forms. In December 1991, when the USSR still formally existed, the first contacts were established with the alliance, and the Russian president declared that he was ready to consider joining it as a “long-term political goal.” Russia was convinced that a new international security architecture would be built together with Europe, which had overcome its ideological split. Moscow was ready for serious steps in the area of arms reduction.

An important event in Yeltsin’s period was the signing of the Charter of Russian-American Partnership and Friendship. It stated, in particular: "The Russian Federation and the United States of America express their commitment to the ideals of democracy, the rule of law and legality, respect for human rights and fundamental freedoms. The United States fully supports the efforts of the Russian Federation to create a democratic state and society based on the rule of law and respect for fundamental human rights (Noori, 2023).

The difficulties of the initial stage of economic reforms led to growing dissatisfaction with the executive branch, and foreign policy was also criticized. Representatives of both the left and right opposition accused the leadership of Russia's loss of independence, influence, its pro-Western orientation, betrayal of former friends and allies, and disregard for national interests (Barsenkov, 2013).

After the Treaty on the Establishment of the European Union (EU) was signed in the Dutch city of Maastricht and entered into force in 1993, Russia acquired a new political and economic partner – a uniting Europe. The usual bilateral ties with European countries had to be supplemented by relations with the EU. In June 1994, the EU-Russia Partnership and Cooperation Agreement was signed, which entered into force in 1997 (Malinova, 2012). This is a truly comprehensive document, covering political dialogue; trade; business and investment; cooperation in the financial and legislative spheres; science and technology; education and training; cooperation in the field of energy, as well as nuclear and space technologies; the environment, transport; culture; cooperation in the prevention of illegal activities. The agreement laid the institutional foundation for cooperation: Russia-EU summit meetings are held twice a year, the ministers of foreign affairs, justice, internal affairs, energy, transport, and ecology meet regularly within the framework of the permanent partnership council, and dialogue is constantly conducted at the level of senior officials and experts. In 1996, Russia joined the Council of Europe, the oldest pan-European organization dealing primarily with legal and human rights issues.

In January 1996, Academician E.M. Primakov became the Minister of International Affairs of the Russian Federation. According to his thoughts, Russian diplomacy had three options: 1) to oppose NATO expansion and refuse any relations with the North Atlantic Alliance; 2) to accept NATO expansion without any attempts to influence this process; 3) to declare a negative position regarding NATO expansion and at the same time conduct negotiations to minimize the consequences that most threaten Russia's security (Rumer, 2019).

Russia chose the third option, focusing on its influence on the expansion process. After almost a year and a half of difficult negotiations, in May 1997, Russia and NATO signed the Founding Act on Mutual Relations, Cooperation and Security in Paris. The document stated that the parties did not consider each other as adversaries (Duleba, 1998). The Founding Act contained provisions that nuclear weapons would not be deployed on the territories of new NATO member countries, and that NATO expansion would not entail "additional permanent stationing of significant combat forces." The act established the NATO-Russia Permanent Joint Council, intended for consultations, development of joint initiatives, adoption of joint decisions, and implementation of joint actions, including participation on an equal basis in the planning and preparation of joint operations. However, although the document was signed by presidents and prime ministers at the highest political level, it was not ratified and was not a legal act. In June 1997, at the Madrid NATO summit, the Czech Republic, Poland, and Hungary were invited to join the alliance. The process of NATO expansion had begun (Garvalho, 1997).

Russia, as the successor state of the former USSR, exercises the rights transferred to it in the international arena. The state lacks the political weight and capabilities that the Soviet Union possessed. However, since the arrival of Vladimir Putin, Russia has been shaped by a paradigm of realism, based on the security of sovereignty and the preservation of the country's territorial integrity. Here, we have to say that all aspects of Putin's foreign policy represent the concept of realism (Vogt, 2024).

The main problems of Russian foreign policy in the late 90s and 2000s of the last century were the weakness of state power and distrust of foreign partners. The attitude of the international community towards Russia was mainly determined by its huge external debt and unstable economic situation. As of January 1, 2000, Russia's public external debt amounted to about 60% of the country's GDP. Creditors, primarily the IMF, doubted that Russia would be able to repay its debts on time. In 2000-2006, the main direction of Putin's foreign policy was precisely to solve the debt problem. During these years, it managed to repay its debts ahead of schedule. This fact significantly increased the level of trust in the new Russian president and the country as a whole. At the beginning of the 21st century, Russia's foreign policy course was aimed at developing bilateral cooperation not only with Western and near-abroad countries, but also with the states of Asia, Africa, and Latin America. In this case, it should be mentioned that Energy diplomacy played an important role (Isajiw, 2016).

V. Putin managed to establish personal and seemingly friendly relations with German Chancellor G. Schroeder, British Prime Minister T. Blair, Italian Prime Minister S. Berlusconi, and found common ground with George W. Bush. It is noteworthy that in 2001, Tony Blair's visit to Russia contributed to improving the international image not only of Putin personally, but also of Russia as a whole (Daddow, 2007).

On January 10, 2000, by decree of the President of Russia, a new concept of Russian foreign policy was approved. The concept outlined the following priorities: the formation of a multipolar system of international relations, strongly opposing the reduction of the role of the UN and the Security Council in world affairs, maintaining a balance between the goals and capabilities of the Russian Federation's foreign policy, solving foreign policy tasks following their real correspondence to the country's national interests (Malinova, 2012).

Thus, in the 2000s, Russia finally managed to return to the forefront of world politics and occupy its niche in the international arena. This is evidenced by the fact that in 2006, the country held the presidency of the G8. It openly declares and consistently defends its national and geopolitical interests. Getting rid of foreign debts and stabilizing the country's domestic political situation allowed the Russian government to confidently defend its position in the dialogue with the West. So, we can say that V. Putin managed to return Russia's lost positions and create a strong and accountable state (Vertlieb, 2021).

Putin faced major foreign policy challenges in 2003-2004. After the Iraq crisis and the color revolutions in Georgia and Ukraine, Russia's foreign policy changed, and it began to take active action (Nygren, 2007). The new approach was no longer based on Soviet methods. By that time, Russia had a new weapon - the economy, and primarily energy resources. The strategic goal of the second phase of Russian foreign policy, which included the period from 2003 to 2006, was economic expansion in the former Soviet territories and thus gaining influence over them (Bacon, 2007).

And in 2003, Russia began to follow the Liberal Empire Theory, formed by Anatoly Chubais, which clearly states that the state must build a new liberal empire from the ruins of the former Soviet Union. For this reason, Russia must promote Russian culture in its neighborhood and ensure the security of the Russian-speaking population. Also, to occupy a dominant position in the trade and business of its neighbors and ensure their independence and democracy. In Chubais' opinion, only in this way will Russia be able to take its natural place in the circle of great democracies, alongside the United States, the European Union, and Japan (Chicherin & Gaidar, 2024).

The main focus is on economic expansion, primarily through the use of energy resources. The main tool of economic expansion used by Putin during this phase of his foreign policy was the state-owned gas monopoly Gazprom. The Russian Energy Strategy, approved by Putin in 2003, makes energy policy the basis of the country's diplomacy (Henderson & Moe, 2024).

Following this policy V. Putin outlined four steps: 1) the Kremlin should not allow European countries to diversify their energy, especially natural gas, supply sources; 2) Russian energy companies should strengthen their control over the international gas market; 3) Russia should control all links in the gas supply chain in the West; 4) the Kremlin should use these assets as a tool of political pressure. Gazprom has focused its efforts on Europe and the main transport corridor - the CIS and Eastern Europe (Solovev, 2006). The European Union covers 60% of its gas consumption through imports, of which almost half comes from Russia. Accordingly, Russia provides more than 25% of Europe's gas supply. It is known that Gazprom owns assets in at least 16 of the 27 EU countries (Rzayeva, 2024).

Putin's speech at the Munich Security Conference in 2007 marked the beginning of the third phase of his foreign policy - active and open confrontation with the West. The recognition of Kosovo's independence, the deployment of US anti-missile systems in the Czech Republic and Poland, and plans to expand NATO further eastward served as catalysts for the beginning of this phase (Buzan, 2024).

In the Munich Security Conference, 2007, Russian President Vladimir Putin accused the United States and other Western powers of undermining global security. Putin’s provocative speech was listened to by 250 officials, including 40 defense and foreign ministers. In a speech couched in harsh terms, Putin criticized the United States for its almost unlimited use of force in the world, He claimed that there is an attempt to create a unipolar world led by the United States, which is unacceptable and dangerous. Putin says that the use of military force is appropriate only in extreme cases, and only under UN sanctions. Thus, we can say that in 2007, Russian President Vladimir Putin's speech at the 43rd Munich Conference, dubbed the "Munich Speech," caused a great resonance in society, and political scientists called it the beginning of a "new Cold War" (Smirnova et al., 2024).

"Munich Speech" was followed by the Russian-Georgian war in August 2008, the loss of Georgia's 20 percent territories, and the so-called recognition of Abkhazia and South Ossetia. Moreover, on June 15, 2009, Russia vetoed the 16-year-old work of the UN observer mission in Georgia, and the annexation of Crimea. After the events in Ukraine in 2014, the Kremlin developed a certain doctrine of Russian foreign and security policy, called Putin's Doctrine about the Russian-Speaking Population and the Use of Military Force in Post-Soviet Space (Shah et al., 2024). According to the doctrine, Russia is the guarantor of the rights of the Russian-speaking population living abroad. This doctrine was applied to the Russian invasion of Ukraine started in February 2022 (Alaverdov & Amilakhvari, 2023).

CONCLUSION

Russia's military actions in Georgia and Ukraine have been demonstrated. First, Russia considers the use of military force in the post-Soviet space to be a legitimate foreign policy instrument. Second, the West has limited resources to deter Russian military actions. Third, Moscow may use the "violation of the rights" of the Russian population in the country as a pretext for military action against neighboring countries.

Thus, we can claim that Vladimir Putin transformed Russia, which was considered a weak successor of the Soviet Union, into a powerful empire. Moreover, he openly accused the world leaders of disrupting global security. After the 43rd Munich Security Conference, the new distribution of the "new Cold War" began, which was followed by the World Order.

REFERENCE LIST

Armscontrol.ru. (2003, May 16). *Treaty on Strategic Offensive Reductions: status, comments, and Expert Views*. Retrieved from https://www.armscontrol.ru/start/rus/sort.htm

Barsenkov, A. (2013). Foreign Policy of Russia at the Initial Stage of the Formation of the New Statehood (1991–1993). *Bulletin of Moscow University*. Series 25. International Relations and World Politics (pp. 75- 105).

Buzan, B. (2024). A New Cold War?: The Case for a General Concept. *International Politics*, 61(2), 239-257.

Burrett, T. (2025). Making Russia Great Again? Vladimir Putin's Changing Sources of Legitimacy 2000–2024. *Politics and Governance*, 13.

Bacon, E. (2007). UK-Russia Political Relations. *The UK and Russia Troubled Relationship*, Part One, (07/17), 13-23.

Chicherin, B., & Gaidar, Y. (2024). Economic Liberals. *Russian Westernizers* *and Change in International Relations: The Promised West*, 87.

Daddow, O. (2007). Playing Games with History: Tony Blair's European Policy in the Press. *The British Journal of Politics and International Relations*, 9(4), 582-598.

De Castro, R. B. (2024). Europe in the World in 2024: From Voting to Geopolitics. *European Policy Centre*.

Glinski, D., & Reddaway, P. (1998). The Yeltsin era in the light of Russian history: reform or reaction?. Demokratizatsiya, *The Journal of Post-Soviet Democratization*, 6(3), 518-534.

Henderson, J., & Moe, A. (2024). *Gazprom: From Rent Distributor to Tax Collector?* Oxford Institute for Energy Studies.

Isajiw, C. P. (2016). Neo-Nationalism in the Foreign Policy of the Putin/Medvedev Regime. *E-International Relations Studies*.

Kennet, W. (2024). *On Ending the Cold War. In The Cold War Past and Present* (pp. 209-223). Routledge.

Laursen, F., & Vanhoonacker, S. (2019). The Maastricht Treaty: Creating the European Union. In *Oxford Research Encyclopedia of Politics*.

Malinova, O. (2012). Russia and 'the West' in the 2000s. *Russia's Identity in International Relations: Images, Perceptions, Misperceptions*, 73.

Nygren, B. (2007). *The Rebuilding of Greater Russia: Putin's Foreign Policy towards the CIS Countries*. Routledge.

Rzayeva, N. (2024). How Gazprom Influenced Decisions in the Foreign Policy of Russia in 2014? (Theory of New Liberalism of Andrew Moravcsik). *Studia Orientalne*, 29(1), 7-16.

Sabry, F. (2024). *European Union: Navigating Integration and Power in a Unified Europe* (Vol. 358). One Billion Knowledgeable.

Solovev, E. (2006). The Foreign Policy Priorities of Liberal Russia. *Russian Politics & Law,* 44(3), 52-72.

Smirnova, Y., Malysheva, O., Aksenov, I., & Tokareva, E. (2024). Speech of Russian President Putin at the Munich Security Conference 2007 ("Munich Speech 2007") as a predictor of the formation of the modern foreign policy agenda of the Russian Federation. *Global Change, Peace & Security*, 1-19.

Shah, M. N. U. H., Abbas, S., & Hussain, I. (2024). Putin Doctrine in Russian Foreign Policy, Challenges for us. *GUMAN*, 7(2), 169-180.

Tripathi, D. (2024). Cold War. In *The Impact of Wars on World Politics, 1775–2023: Hope and Despair* (pp. 37-53). Cham: Springer Nature Switzerland.

Vogt, H. (2024). Relations EU-Russia: a Paradigm Shift. *EU Enlargement and European Integration: Challenges and Perspectives*, p.161.

Vertlieb, E. A. (2021). Project Putin-2024 in the Geostrategy of Confrontation and Internal Challenges. *Security and Intelligence*, 6(2).

Matthieu Grandpierron[1]

THE DANGER OF ARTIFICIAL INTELLIGENCE AND POSITIVISM TO UNDERSTAND STRATEGIC POSITIONING

Abstract

The development of artificial intelligence has opened up doors both for research and for strategic uses. With its capacity to quickly analyze and put together important and complex datasets, AI has been seen, especially in the West, as a solution to analyze complex and fast- changing situations. While offering answers, the use of AI in the field of strategic anticipation is not exempt from limitations. One of the most important is its positivist and euro-centric dimension. This raises the question of whether concepts derived from a particular political and cultural context (Europe) are suitable for truly understanding the realities of different cultures and civilizations. The answer seems obvious; Martin Wight (1977) and Barry Buzan (1977) have often denounced these risks. Surprisingly, they have not been heard. This article will examine all these issues and link them to the question of research methodology, particularly the use of positivism as a source of inspiration for research methods. By treating history as a set of data and civilizations as variables, positivism creates the conditions for Eurocentrism. This article concludes by proposing an alternative research method that aims to avoid cultural bias as much as possible when carrying out comparative studies.

Keywords: *Positivism, Euro-Centrism, Strategic Anticipation, AI, Predictive Politics.*

INTRODUCTION

Artificial Intelligence has emerged as a key tool for policymakers, intelligence agencies, and decision-makers, offering data-driven insights into economic trends, military developments, and geopolitical shifts. The capacity of AI to process vast amounts of data in real-time has made it an attractive tool for strategic anticipation, particularly in the West, where positivist methodologies have dominated foreign policy analysis since Kenneth Waltz influential 1959's book. AI-based models promise objective, empirical, and scientifically rigorous analyses to better understand complex situations and predict what other actors are likely do in a given situation. Yet, they also bring forth deep methodological and empirical challenges and risks. In a fast-evolving context that

[1] Catholic University of Vendée (ICES), France, m-grandpierron@ices.fr

sees the West being increasingly challenged geopolitically, economically, and with the legitimacy of its international order more and more contested, AI has been regarded as an ideal tool for navigating and making sense of uncertainty, anticipating perceived threats and stopping the erosion of the Western dominant position. AI thus appears as the miracle solution to predict behaviors (Sinha, 2024; Mirahmadi & Omidi, 2024), acting just like the precogs in *Minority Report*.

However, while AI offers new possibilities in strategic anticipation, its use is not without significant limitations. One of the primary issues is AI's inherent reliance on positivism, the philosophical approach that seeks to explain political and historical events through empirical laws and quantifiable patterns. This approach assumes that complex sociopolitical behaviors can be measured, categorized, and predicted using statistical models. While such a methodology may be useful in analyzing certain trends, it is highly problematic when applied to strategic positioning and foreign policy, as it often disregards historical contingencies, cultural nuances, and ideological differences that shape political behavior.

The second issue is Eurocentrism, a structural bias embedded within AI training datasets and analytical frameworks. AI models are often developed using Western political theories, historical experiences, and epistemological assumptions, leading to a distorted interpretation of non-Western strategic behavior (Shawon, Dalim, and Shil, 2024). This results in misreading geopolitical events, overestimating military threats, and misjudging diplomatic intentions.

The Western tendency to rely on positivism and to stick to Eurocentrist thinking is likely to be reproduced in and by Western AI tools, thus continuing to shape Western decision- makers' decisions and understandings of the world based on these biases. AI models, largely trained on Western political and historical experiences, often misinterpret non-Western strategic behaviors, leading to flawed assessments of geopolitical actors such as China. This raises the following question: Are AI models, largely built upon Western political and cultural assumptions, capable of accurately understanding the strategic realities of different civilizations?

This paper critically examines how positivism and Eurocentrism limit AI's capacity to accurately interpret strategic positioning. It explores how these biases shape AI-driven foreign policy analysis, leading to flawed strategic assessments. The final section proposes alternative methodologies to correct these biases, advocating for a more context-sensitive and historically informed approach to AI-driven strategic forecasting.

WESTERN APPROACH TO FP: POSITIVISM AND EUROCENTRISM

Positivism and the risk to create one-model to fit-all situations

Positivism grew out of a movement to establish a sound basis for social science enquiry in relation to natural law (Strauss, 1953). Political research wants to provide credible answers to important questions and needs to ensure that the research practices and methods it employs allow it to do so. Positivism proposes an approach to solving this problem: it asserts that researchers can arrive at factual, reliable and objective answers to questions about the social world by employing the methods used in the natural sciences (Durkheim, 1963). The term positivism was coined by Auguste Comte (2021) to describe the last of the three phases through which society passes in its search for truth. According to Comte, society had passed through a theological stage, then a metaphysical one, and had entered a final "positive" stage in which the search for truth is characterised by the systematic collection of observed facts.

Other principles of positivism flesh out this position: the aim of the social sciences is to explain and predict social phenomena by means of laws. Carl Gustav Hempel (1965) argued that if the discovery of laws is necessary in the physical or natural sciences, then laws must also be necessary in the social sciences: if the social world is like the natural world, then, like the natural world, it must be regular, systematic and governed by laws; there are regularities in social and political processes, and we can explain social events and phenomena by means of law-like generalizations that have the same status as natural scientific laws.

Quantitative research in political science largely consists of what are known as 'large- n studies'. The quality of the research depends to a large extent on the observation effort and raises the question that every researcher asks: How many cases should we study, how many people should we interview? By multiplying observations and sources, confidence in the results is increased because it is easier to generalize what is repeated. When the data is quantitative, the greater the number of observations, the better the conditions for refutation based on statistical estimation methods. The disadvantage is that quantitative research methods ignore specificities such as culture, political philosophy and history. As a result, they lead to abusive generalizations, attributing to actors claims that are not necessarily true.

Positivism applied to the political science research method has contributed to setting aside the factors of human behavior long identified by Thucydides (2000). Thus, perceptions and emotions have been regarded as unscientific and not worthy of being an object of research.

When emotions have been taken into account in analyses of international relations, they have often tended to be studied from a utilitarian, or at least rationalist, point of view (Jervis, 1976; Janis, 1982). Morgenthau (1946) was partly responsible for this, no doubt in spite of himself, by including fear in the highly rationalist model of nuclear deterrence. Following the work of Kenneth Waltz (1959), emotions were set aside because their impact could not be studied and quantified scientifically using the positivist methodology of the social sciences. The study of emotions involves studying those who feel and express them. What is the point of focusing on a single man, even the president of the world's leading power? How can his 'personality' be useful in understanding international processes? This brings us face to face with the thorny problem of individual causality. How can we be sure that what we attribute to emotions is not ultimately a convenient mask behind which we will always find material or symbolic advantages? Under what circumstances do emotions become shared, public and political?

Answering these questions is not easy. It is much easier, as neo-realists do, to rely solely on material factors and databases to predict state behavior. For many positivist security researchers, international actors are driven by external forces that push them in a particular direction (Mearsheimer, 2014), or future threats are deduced from past trends, as if the social world were advancing in a linear fashion (Colonomos, 2016). In both cases, these analyses suffer from major problems. Firstly, they completely overlook the differences between civilizations, their histories, cultures and political philosophies. Secondly, if examples are drawn from the past, they are all taken from European history, thus participating in the movement to create a homogeneous positivist world based solely on European history and values.

This approach evacuates all subjectivity, social ties and emotions in social relations. Positivism makes us imagine the worst-case scenario (Lindemann, 2023): This is especially true in hardcore realism and liberalism. Hardcore realists will argue that war is inevitable and thus contribute to creating unnecessary alarmism. This alarmism assumes rational, self-interested and strategic actors struggling for power and resources. This alarmism is rational insofar as the threatening actions are not attributed to actors driven by passion or revenge, but to cold self- interest or historical forces. A current argument in West-European and North American literatures are what they call the China Threat or the Russian Threat (Rojelja & Tsimonis, 2020). These countries are often presented as homogeneous actors that "rise" and appear to be intent on imposing its will on the world in a near future through a long-standing strategic plan.

Hard-line liberals are of exactly the same opinion: war is no longer possible and will never happen (Mueller, 1990), particularly because Western values 'won' the Cold War.

Consequently, any non-European country will automatically aspire to become like the Europeans and apply the European conception of democracy and human rights (Fukuyama, 2020). Democracies are always peaceful, while non-democracies are always violent (Russett, 1994). As such, a 'democracy' can only be a political construct corresponding to the Euro- Atlantic conception. Any other model is not a 'true' democracy, cannot be described as such, and is in fact an attempt by corrupt elites to manipulate it in order to pass itself off as a democracy. The conclusion is to assume that cultures, histories and civilizations are all equal. In this competitive universe, there is no room for real cooperation, social ties or anything related to the development of a new international order (Ikenberry, 2014; Sahakyan & Gärtner, 2022; Sahakyan, 2023).

Positivism denies any room for heterogeneity, creativity and social connections between actors (Benetton, 2017). Firstly, with regard to the subject, positivist approaches in IR have a mainly homogenizing and aggregative approach to subjects that denies individuality. While certain categorization and typification are necessary for any science to 'know' certain aspects of social reality, nomological positivism tends to reify these categories and, for example, personify aggregations with given interests and emotions, such as the desire for 'Chinese' dominance. Structural positivist researchers tend to deny subjects in an aggregated whole, leading to the reification of actors collective. This unification can make actors appear particularly powerful and dangerous. If actors are perceived as unified, such as "Russia", "China", "North Korea" or "Iran", it becomes easier to attribute a coherent will to them (Lindemann, 2023). It is often forgotten that foreign policy actions are more often the result of compromise than of coordinated policy. In their discourses and narratives, Western countries use a new form of positivist Eurocentrism that is a continuation of this process. They combine positivism with Eurocentrism to further deny the possibility of a heterogeneous world.

Eurocentrism and the attempt to create a world that rejects heterogeneity

Western approach to politics is based on the interpretation that the West won the Cold War (emphasis is put on the idea of victory, not on the fact that the USSR collapsed). As such, not only the West got prestige, but it also gained certainty that the western model was the ultimate stage of human development. This is what Fukuyama (2020) argued. This neo-Kantian position assumes that individual states with democratic political regimes constitute an ideal that the rest of the world will follow. The projection of the principles of liberal democracy to the field of IR combined with a positivist logic offers the best future for a peaceful world order: the more democracies there are, the more peaceful the world will be; the fewer democracies there are, the less peaceful the world will be. Liberals believe that the legitimacy of the domestic political order is largely down to respect for the law and the state's respect for human rights. If it is wrong for individuals to commit criminal or socially unacceptable acts, then it is also wrong for states.

This creates a sense of superiority and revives the colonial belief that the West was once again the center of civilization. Liberal ideology makes it hard for liberal leaders to accept any contestation or power sharing, whether at home or on the international scene. This is reflected in how Western actors and decision-makers understand the world. To them, it is self-understanding that any concept has to be understood and defined based on Western standards. They reject the possibility that Human rights can be defined differently than the way are in the West. If in the West, Human rights are understood as individual rights that the individual enjoys to project itself from the West, in other cultures, such as in China and in the Global South, Human rights are understood as economic rights. Such different understandings lead to unnecessary tensions that could easily be solved if Western leaders accept the idea that there exists a heterogeneity of cultures and understandings.

The same applies to international relations concepts. The dominance of neo-realism I Western approach to international relations leads to the understanding that power can only be understood as in the Western sense and that the path to great power status consists in replicating the path taken by the US following WWII (Mearsheimer, 2014). This logic is highly deterministic as it is solely based on US history. Such logic falls into the shortcomings identified by Martin Wight (1977): The absence of historical and philosophical contextualization leads towards uniformity of behavior.

In their discourses and narratives, Western countries use a new form of positivist eurocentrism that is the continuation of the process discussed in this paper. They combine positivism with Eurocentrism and biopolitics to further deny the possibility of a heterogeneous world. They put forward a self-proclaimed moral and institutional superiority of democracy would give it the right to manage world affairs and to sanction any deviant behavior (de Broux, 2019). This criterion of leadership is often the justification for the 'humanitarian intervention' policies of democracies (Wheeler, 2000; Chesterman, 2001; Orford, 2013; Tesón, 2005). Because the West has enhanced moral and behavioral superiority, Western leaders argue that they are 'fit to lead' the world because of their self-proclaimed superior political regimes, and give them the de facto "right" to punish or reward non-Western countries for their behaviors.

The combination of positivism and Eurocentrism makes Western decision-makers live in a past that not only no longer exists, but that is also no longer desired by the vast majority of countries (Perembroke, 2021). Such discourses are also performed at the international level through a manipulative use of international law. International law is an instrument of power. It is even more than that; it is actually understood as a language, with a grammar and a lexicon that reconstitute the discourse and have an impact on those who are deemed capable of claiming to speak the law. For liberal democracies, it is obvious that the international community can only be composed of liberal democracies and therefore consider any other form of regime as illegitimate (Kühnhardt, 2017;

Pabst, 2019; Parsi, 2021; Sørensen, 2011). Sanctioning would therefore allow the construction of a world composed exclusively of liberal states and, ultimately, dissolve the distinction between liberal democracies and international society (Buchan, 2013).

FLAWED WESTERN AI: HOW THE USE OF TECHNOLOGY REINFORCES WESTERN INABILITY TO CORRECTLY UNDERSTAND OTHERS

Perpetuation of Western-centric models in and by AI

Western-trained AI models frequently fail to interpret non-Western political behaviors accurately because they are built on Western historical experiences and theoretical paradigms. The dominance of European and American political thought in AI model development creates structural biases that misinterpret how different civilizations approach power, diplomacy, and conflict resolution (Menkel-Meadow & Schneider, 2025; Khan, 2025).

AI-driven predictive models rely on data mining, pattern recognition, and probability analysis to anticipate state behavior. While these methods may be effective in areas such as economic forecasting or logistical planning, they struggle to predict political decisions influenced by historical grievances, ideological considerations, and leadership psychology (Radanliev, 2025). For example, AI models that attempt to predict China's foreign policy often fail to account for Confucian strategic patience, the historical memory of Western imperialism and imposed humiliations, and the way the Chinese Communist Party works in shaping decision-making. Instead, AI applies Western frameworks of power competition, leading to misreadings of China's actions and decision-making processes, concluding that China is an expansionist and aggressive power.

Western AI models operate on the premise that historical data can be used to anticipate future developments, yet strategic positioning is not a mechanistic process. It is shaped by human agency, ideological considerations, and culturally specific logics that cannot always be quantified (Zaabar, Razali, Ishak, & Abdullah, 2024). By treating history as a dataset and civilizations as quantifiable variables, AI models create a false sense of objectivity in strategic analysis. However, history is often context-specific and shaped by unique sociopolitical factors. AI models that rely on historical trend analysis tend to overgeneralize patterns, leading to inaccurate predictions and flawed risk assessments.

Western-trained AI models frequently fail to interpret non-Western political behaviors accurately because they are built on Western historical experiences and theoretical paradigms. The dominance of European and American political thought in AI model development creates structural biases that misinterpret how different civilizations

approach power, diplomacy, and conflict resolution. For instance, AI- based risk assessments often overstate the probability of military conflict by relying on past patterns of war initiation while ignoring diplomatic maneuvers, internal political debates, and economic interdependencies that act as conflict deterrents.

Most AI models are trained using datasets that disproportionately reflect European diplomatic history, Cold War geopolitics, and liberal democratic institutions. This skews AI predictions by treating these historically contingent experiences as universal models for international relations. When applied to non-Western states, these models often misdiagnose strategic behaviors, leading to policy miscalculations. Western political traditions emphasize clear treaty obligations, explicit diplomatic commitments, and defined spheres of influence (Cohrs, 2022). In contrast, many non-Western cultures prioritize ambiguity, flexibility, and indirect communication in international relations. AI models struggle to process these nuances, as they are programmed to identify binary outcomes and direct causal relationships. For example, Western AI-driven analyses of China often categorize the Belt and Road Initiative (BRI) as neo-imperialism, failing to consider its roots in China's historical trade diplomacy and Confucian concepts of hierarchical order (Ford, 2015). Similarly, AI predictions about China-Russia relations tend to assume a transactional alliance, overlooking the deeper historical narratives of mutual distrust and pragmatic cooperation that shape their partnership.

Western AI trained on dichotomous theories

When asking Western AI to propose strategic and geopolitical understanding, most of the results generated are based on two deterministic and dichotomous theoretical approaches: liberalism and neo-realism.

AI models that are trained on liberal theories such as democratic peace theory (Russett, 1994) operate under the premise that increased economic interdependence will result in democratic governance. When a country does not conform to this expectation, AI-driven forecasts often flag this divergence as an anomaly or a sign of authoritarian entrenchment, rather than recognizing a different governance model as a distinct and historically rooted political structure. This leads to repeated policy miscalculations, as Western strategies often assume that economic pressure or sanctions will drive political reform, despite repeated evidence that non-Western countries remain resilient (Mudler, 2022).

Another limitation is the Cold War-era framing of international relations, which influences AI models trained on realist balance of power theory. These models frequently classify a country's rise as inherently adversarial to the existing international order, interpreting its economic growth, military modernization, and global infrastructure projects as direct threats (Gilpin, 1981; Taliaferro, 2004). AI forecasts that rely on

Cold War patterns tend to treat any Chinese foreign policy initiative – such as the Belt and Road Initiative or regional security pacts – as an attempt to establish a hegemonic order rather than as a form of economic diplomacy. This results in alarmist intelligence reports that exacerbate Western fears about China's intentions, prompting aggressive countermeasures that escalate tensions rather than resolve them.

In the context of the changing world, constructivism provides a way of thinking that helps escape positivism and Eurocentrism by reestablishing the importance of emotions (Saurette, 2006; Grandpierron, 2024), and contextualized and cultural understanding of political phenomena (Wendt, 1999). Such approach is particularly required to understand changes and will to change the international order without seeing it as a casus belli (Paul, 2015; Acharya, 2025). In addition, AI models often struggle with constructivist approaches to foreign policy, particularly when analyzing the role of national identity and historical memory in China's diplomatic strategy. Unlike Western nations, which frequently engage in explicit alliances and treaty-based diplomacy, China often communicates through historical references, symbolic gestures, and indirect diplomatic signaling. AI-driven analysis often misinterprets these signals, as it is trained to detect explicit policy declarations rather than subtle forms of communication. As a result, China's foreign policy maneuvers are often misclassified as unpredictable or contradictory when, in reality, they are guided by a long-term strategic vision that is deeply embedded in China's historical experiences.

MISINTERPRETING NON-WESTERN ACTORS: THE CASE OF MAKING UP "THE CHINA THREAT" AND "THE COLD WAR MENTALITY"

Western liberal thinkers, particularly those of the triumphant post-Cold War era, have chosen to conform to a rather algorithmic vision of national success. For them, there is a perfect political system - governance software - which, if downloaded and installed, would automatically ensure national success. Indeed, in 1991, academics and politicians were adhering to a triumphant school of thought that prophesied the end of history based on the socio-economic software provided by the great victor of the Cold War, the United States. The rest of the world had to conform to the institutional ethos put in place by America if it wanted to develop economically or risk stagnation and perpetual poverty.

Researchers from the Global South and non-Western countries are struggling to make their voices heard. Nor do they often take part in prestigious international conferences or have their research published by well-established academic publishers. Consequently, the issue of comparing political systems, political philosophies, worldviews, and international issues suffers from a major limitation: it is carried out more or less exclusively by Western academics and/or using mainly Western political concepts and research methods. This raises the question of whether concepts derived from a particular political and cultural context (Europe) are suitable for truly understanding the realities of different cultures and civilizations.

China's foreign policy has long been characterized by strategic ambiguity, allowing it to maintain flexibility in negotiations and conflict scenarios. However, AI struggles to differentiate between strategic ambiguity and genuine military intentions, leading to misinterpretations of China's geopolitical strategy. One of the clearest examples of this misinterpretation is China's position on Taiwan. AI models trained on Western military conflict patterns frequently predict imminent invasion scenarios when analyzing Chinese military maneuvers around Taiwan. However, China's Taiwan strategy is primarily economic and political rather than military-driven. AI models, trained to identify military buildups as precursors to war, fail to recognize China's preference for economic coercion and cyber influence over direct military action. They overestimate the likelihood of direct military confrontation based on Cold War patterns and fail to account for China's long-term economic and diplomatic strategies that reduce the need for military conflict.

Similarly, AI models have misinterpreted China's stance on global conflicts, such as Russia's invasion of Ukraine. AI-driven Western assessments often misinterpret China's non-committal stance as implicit military support for Russia. In reality, China's ambiguous positioning is a diplomatic strategy aimed at maintaining economic ties while avoiding direct entanglement. AI, lacking the ability to interpret diplomatic subtleties and indirect signaling, misrepresents China's actions as either aggressive or duplicitous. For example, AI assessments of China's Belt and Road Initiative frequently classify it as neo-colonial expansionism (Larkin, 2022; Shawon, Dalim and Shil, 2024), whereas Chinese policymakers frame it as an economic interdependence strategy. AI models, lacking a nuanced understanding of China's diplomatic philosophy, reinforce alarmist narratives that lead to aggressive Western countermeasures such as trade wars and economic sanctions (Lee, 2024).

CONCLUSION:

AI has the potential to revolutionize strategic forecasting, but its current methodological limitations pose serious risks to international stability. The use of AI in strategic positioning and predictive politics is not neutral; it is shaped by positivist methodologies and Eurocentric biases that distort how non-Western states are analyzed. By reducing history to quantifiable datasets and civilizations to predictive variables, AI reinforces misinterpretations that drive flawed policy decisions. To avoid these pitfalls, AI-driven geopolitical analysis must integrate historical context, non-Western strategic thinking, and human interpretative expertise to produce more accurate and balanced assessments of global affairs.

To mitigate the biases in AI-driven strategic analysis, it is necessary to adopt more culturally informed methodologies. AI models must be trained with non-Western political theories, historical frameworks, and diplomatic traditions. This would allow AI to process a broader spectrum of strategic behaviors, reducing misdiagnosed geopolitical risks. Moreover, AI's predictive assessments should be complemented by human geopolitical expertise. AI alone cannot interpret the cultural, ideological, and historical factors that influence foreign policy decisions. By integrating AI-driven data analysis with qualitative expert evaluation, policymakers can develop more balanced and contextually accurate foreign policy responses.

REFERENCE LIST

Acharya, A. (2025). *The Once and Future World. Why Global Civilisation will Survive the Decline of the West,* London: Basic Books.

Bénéton, P. (2017). *Le Déréglement Moral de l'Occident,* Paris : Le Cerf.

Buchan, R. (2013) *International Law and the Construction of the Liberal Peace*. Oxford: Hart Publishing.

Chesterman, S. (2001). *Just War or Just Peace ? Humanitarian Intervention and International Law.* Oxford: Oxford University Press.

Colonomos, A. (2016). *Selling the Future. The Perils of Predicting Global Politics*, Oxford: Oxford University Press.

Cohrs, P. (2022). *The New Atlantic Order: The Transformation of International Politics 1860- 1933*. Cambridge: Cambridge University Press.

Comte, A. (2021). *Discours sur l'Esprit Positif.* Paris: Garnier.

de Broux, P-O. (2019). Nations civilisées, mission civilisatrice, droit de civilisation. *Revue Interdisciplinaire d'Etudes Juridiques* 83(2): 35–49.

Durkheim, E. (1963). *les Règles de la Méthode Positiviste*. Paris : PUF.

Ford, C. (2015.) *The Mind of Empire: China's History and Modern Foreign Relations.* Lexington: University Press of Kentucky.

Fukuyama, F. (2020). *The End of History and the Last Man.* London: Penguin Books.

Gilpin, R. (1981) *War and Change in World Politics.* Cambridge: Cambridge University Press.

Hempel, C. (1965). *Aspects of Scientific Explanation and other Essays in the Philosophy of Science*. Amsterdam: Free Press.

Ikenberry, J. (2014). *Power, order, and change in world politics*. Cambridge: Cambridge University Press.

Janis, I. (1982). *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*. Boston: Houghton Mifflin Co.

Jervis, R. (1976). *Perception and Misperception in International Relations*. Princeton: Princeton University Press.

Khan, A. (2025). Redefining Conflict in the AI Era: Transforming Paradigms in International Security, *Al-Aasar*, 2(1): 1-14.

Kühnhardt, L. (2017). *The Global Society and Its Enemies : Liberal Order beyond the Third World War*. Cham: Springer.

Larkin, T. (2022). China's normfare and the threat to human rights. *Columbia Law Review*, 122(8), pp.2285–2322.

Lee, K. (2024). *Researching the Belt and Road Initiative. A Cross-Civilisational and Interdisciplinary Approach*. New York: Springer.

Lindemann, T. (2023). Theorising Danger or Dangerous Theories? Positivist Data and the Making of the China Threat. *Political Anthropological Research on International Social Science*, 4: 142-172.

Mearsheimer, J. (2014). *The Tragedy of Great Power Politics*. New York: W.W. Norton and Company.

Menkel-Meadow, C.; Schneider, A. (2025). International Conflict Resolution Processes. Carolina Academic Press, *UC Irvine School of Law Research Paper* No. 2025-06, Available at SSRN: https://ssrn.com/abstract=5168799 or http://dx.doi.org/10.2139/ssrn.5168799

Morgenthau, H. (1946). *Scientific Man Versus Power Politics*. Chicago: University of Chicago Press.

Mudler, N. (2022). *The Economic Weapon. The Rise of Sanctions as a Tool of Modern War*, New Haven, Yale University Press.

Mueller, J. (1990). The obsolescence of major war. *Bulletin of Peace Proposals,* 21(3), 312- 328.

Mirahmadi, S. & Omidi, A. (2024). Applications of Artificial Intelligence in Foreign Policy Decision-Making: Capacities and Challenges. *Political Strategic Studies*, 13(50), 259- 300

Orford, A. (2013). Moral Internationalism and the Responsibility to Protect. *European Journal of International Law,* 24(1): 83–108.

Pabst, A. (2019). *Liberal World Order and Its Critics: Civilisational States and Cultural Commonwealths.* London: Routledge

Parsi, V. (2021). *The Wrecking of the Liberal World Order.* Cham: Palgrave Macmillan

Paul, T.V. (ed.) (2016). *Accommodating Rising Powers. Past, Present and Future.* Cambridge: Cambridge University Press.

Perembroke, R. (2021). *America in Retreat. The Decline of US Learship from WW2 to COvid-19*. London: OneWorld Books.

Radanliev, P. (2025). Frontier AI Regulation: What Form Should It Take?.999999*Front. Polit. Sci.* 7:1561776. doi: 10.3389/fpos.2025.1561776

Rojekja, I.; Tsimonis, K. (2020). Narrating the China Threat: Securitizing Chinese Economic Presence in Europe. T*he Chinese Journal of International Politics*, 13(1), 103-133.

Russett, B.M. (1994). *Grasping the Democratic Peace: Principles for a Post-Cold War World*. Princeton: Princeton University Press.

Sahakyan M.; Gärtner H., (eds.) (2022). *China and Eurasia: Rethinking Cooperation and Contradictions in the Era of Changing World Order*. New York: Routledge.

Sahakyan M., (ed.) (2023). *China and Eurasian Powers in a Multipolar World Order 2.0: Security, Diplomacy, Economy and Cyberspace*. New York: Routledge.

Saurette, P. (2006). You dissin me? Humiliations and Post 9/11 Global Politics. *Review of International Studies*, 32(3): 495–522

Shawon, R., Dalim, H., & Shil, S. (2024). Assessing Geopolitical Risks and Their Economic Impact on the USA Using Data Analytics. *Journal of Economics and Political Studies*, 6(6): 5-16.

Sinha, G. (2024). AI-Driven Forecasting Models for Anticipating Oil Market Trends and Demand. *International Journal of Artificial Intelligence and Machine Learning*, 6(6).

Sørensen, G. (2011). *A Liberal World Order in Crisis: Choosing between Imposition and Restraint*. Ithaca, N.Y: Cornell University Press

Strauss, L. (1953). *Natural Right and History*. Chicago: University of Chicago Press.

Taliaferro, J.W. (2004). Power Politics and the Balance of Risk: Hypotheses on Great Power Intervention in the Periphery. *Political Psychology*, 25(2): 117–211

Tesón FR (2005) *Humanitarian Intervention : An Inquiry into Law and Morality*. New York: Transnational Publishers

Thucydides, (2000). *La Guerre du Péloponnèse*. Paris : Folio.

Waltz, K. (1959). *Man, State and War.* New York: Columbia University Press.

Wendt, A. (1999). *Social Theory of International Politics*. Cambridge: Cambridge University Press.

Wheeler, N.J. (2000). S*aving Strangers Humanitarian Intervention in International Society.* New York: Oxford University Press.

Wight, M. (1977). *Systems of States*. (Edited by Hedley Bull). Leicester : Leicester University Press: 21-46.

Zaabar, L. , Razali, N., Ishak, K., & Abdullah, N. (2024). A Review on Deep Learning Approaches and Optimization Techniques for Political Security Threat Prediction. *Journal of International Security Studies,* 8(3): 1082-1090.

Rejani Thudalikunnil Gopalan[2]

TERRORISM: CHALLENGES AND WAYS TO HANDLE IT IN THE MODERN WORLD

Abstract

One of the major threats to human existence is terrorism and it is spreading like a pandemic and almost every country in the world faces its tragic and horrible consequences. In general way it can be define that terrorism is an action or threat to influence the government or intimidate the public for a political, religious or ideological reason. The impact of terrorism is not limiting to the political atmosphere but it touches almost all aspects of life which placing the world in the shadow of fear and anxiety. It poses threats to the security of the individual, nation and world at large. Though many countries are aware of the negative influence of terrorism, they are struggling to handle the terrorism effectively due to its associated complexities like economical source and technological advancements. This paper mainly focuses on the challenges posed by terrorism and ways to handle terrorism at multilevel strategies and the importance of multinational security system collaborations.

***Keywords**:Terrorism, Causes of Terrorism, Ways to Handle Terrorism, Forensics.*

The modern world faces lots of threats and crises to its existence, and one of such is terrorism. Over the years, the complexity of terrorism has increased, and it has spread like a pandemic, and almost every country in the world faces its tragic and horrible consequences. In a general way, it can be defined that terrorism is an action or threat to influence the government or intimidate the public for a political, religious, or ideological reason. The impact of terrorism is not only the loss of life and property damages, but also psychological damages that last for years. It touches almost all aspects of life, placing the world in the shadow of fear and anxiety. It threatens the security of the individual, nation, and world at large. Dealing with terrorism or counter-terrorism poses huge challenges at national and international levels due to its complexities, and this article explores its challenges and possible remedies.

Terrorism and the challenges to deal with it:

To prevent or deal with terrorism, many strategies and steps have emerged at the national and international levels and continue. Though many rules and regulations came into play, the preventive methods are still in preliminary stages or not as effective as expected, and many factors are hindering them. The article mainly focuses few hindering

[2] Apex University, Jaipur, Rajasthan, India, rejanigopal@yahoo.co.in

factors or challenges, like issues in definition, financial sources, money laundering, and the use of technologies in the operation of terrorism, especially in the financial matters.

(a) Problems in the definition of terrorism:

The common features of the definition of terrorism include terror or instilling fear, and violence. Unfortunately, there is no consensus over the definition of terrorism internationally, and every nation has its own definition, which may contradict others. For example, according to The UN Security Council (UNSC) (2004) terrorism is defined as “criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act” (Resolution 1566). It emphasizes that it is a criminal act to generate fear to obtain something. As per FBI, “Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.” This definition mainly focuses on the motive of terrorism to gain something politically or socially. The U.S. Department of State defines terrorism to be “premeditated politically-motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience”. The focus of the definition of a very thoughtful political motive to influence by violence. While above mentioned definitions focused either on criminalization of the violence or motives of the violence, the definition given by the European Union provides a more comprehensive definition, emphasizing more clarity on the acts or criminal offences. It defines that terrorist offences are certain criminal offences set out in a list consisting largely of serious offences against persons and property that given their nature or context, may seriously damage a country or an international organization where committed with the aim of: seriously intimidating a population; or unduly compelling a Government or international organization to perform or abstain from performing any act; or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization.

When there is no consensus among the definitions of many countries and organizations, it is difficult to implement the law and order internationally. The act may be criminal in one nation but may be justified in another country, which will hamper the implementation of counter-terrorism activities like exchanging terrorists between countries or banning terrorist groups. Not only do the words terrorism and terrorists need clarification, but also the activities under the umbrella of terrorism, and that again creates clashes among the nations. Lack of a definition may facilitate the politicization and misuse of the term "terrorism" to curb non-terrorist (or sometimes even non-criminal) activities which can result in States, e.g., violating the rights of their own or other States' citizens, such as those of international human rights law, in the course of their counter-terrorism efforts (UNODC). According to Sorel (2003), to define terrorism globally, a clear distinction needs to be made between how the act was undertaken and its consequences, by whom the act was perpetrated, and the reason why the act was committed. Clarity in definition can make the strategies easy for the nations to restrict or to take criminal action against terrorism.

(b) Identification of economic resources:

The second issue related to handling terrorism is the identification of the economic resources and their restrictions. Terrorist activities need funds, which many of the terrorist organizations arrange through legitimate or illegal means. They derive money by using NGO's, charitable organizations, or doing business, and in the worst scenario, by kidnapping, drug trafficking, and even using natural mineral resources. Terrorists use money to pay for their material needs and activities, ranging from organizational needs such as food, water, logistics, and salaries to preparing terrorist attacks; to move funds as part of their financing activities and they store and manage the funds that they obtain, either for organizational or operational purposes (Davis,2021).

The exchange and transfer of these funds within a nation and across nations uses formal and informal financial systems, and terrorists use the most advanced way of money transfer, and they are up to date with technologies and keep changing the methods of transferring. Terrorist organizations sometimes even take money in small donations instead of huge amounts to evade the rules and regulations of the country. The money laundering of dirty money to finance terrorism follows many calculated steps. According to Sorel (2003), to invest the dirty money in to financial system, large amount divides in to small amount of cash and put them in to different bank accounts in different banks and different places, and these amounts may be moved to different accounts or use for payment of goods or services to make it 'clean money'. After this, they integrate these funds into legal economic activities. Aninat, Daniel and Johnston (2002) explained the laundering of money in a more precise way, such as cash is derived from criminal activities or similar activities deposited in banks by people who are not involved in these crimes, then split these amounts to small amounts to smurfs or agents which is called layering. Also, they create misleading paperwork, which makes it easier to disperse the funds abroad.

Steps against Money Laundering and the Financing of Terrorism

Many steps and strategies were initiated to fight against terrorism, and several national and international conventions and activities happened, especially to fight against money laundering and financial support for terrorism. The 1988 Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, The Strasbourg Convention, The Organization for Economic Cooperation and Development's Convention on Corruption, The Palermo Convention Against Transnational Organized Crime, The Convention for the Suppression of the Financing of Terrorism and the activities like 40 recommendations of the FATF, blacklisting the organizations, The European Directives of 1991 and 2001, The Naples Action Plan and The New York Action Plan are the major conventions and activities happened to battle against the financial support for terrorism. The 1988 Convention emphasised the fight against organized crime and drug trafficking in the view that financial profits from these activities are used for terrorism like activities and The Strasbourg Convention made a step ahead to make rules for preventing money laundering in the banking and financial system and also sought international cooperation for seizure and confiscation of illicit money and recommended mutual judicial assistance in investigations. In 1999, the Organization for Economic Cooperation and Development's Convention on Corruption implemented the rules to prevent corruption in international trade, and the Organization for Economic Cooperation and Development (OECD) was given the responsibility to monitor the activities. While making laws against Transnational organized crime was the focus of the Palermo Convention Against Transnational Organized Crime, the primary focus of the Convention for the Suppression of the Financing of Terrorism was to make an international strategy against the financing of terrorist activities. The G-7 Summit in 1989 resulted in 40 recommendations for FATF (Financial Action Task Force on Money Laundering) to handle money laundering, and eight new recommendations were added to fight against financing of terrorism after the attacks of September 11, 2001. The European Directives of 1991 and 2001 have resulted in legislation to prevent money laundering and apply to all states of the European Union. The Naples Action Plan and The New York Action Plan focused on strategies to prevent money laundering at the international levels. All these conventions made landmarks in the creation of steps and strategies to handle money laundering and dirty money to finance terrorism at the international level. But major actions or importance of these conventions and strategies got more limelight after the attack on 23 September 2001in the USA, and more rules and regulations were implemented. In the latest development, the United Nations Security Council Counter-Terrorism Committee adopted the "non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies. This declaration was made on 6th January 2025 which is known as Algeria Guiding Principles.

Though conventions and meetings drafted many regulations to handle financing terrorism, it is not as effective as planned. The restrictions imposed to restrict financial resources for terrorism may require more structured planning and scrutiny. For example, Al Qaeda's ability to operate with financial resources runs smoothly even after restrictions. As mentioned by Basile (2004), the reasons could be many, such as Al Qaeda has built a strong network of financiers and operatives who are both frugally minded and business savvy, and thus terrorist finances are often hidden in legitimate and illegitimate businesses and disguised as commodities and cash. They also learned to effectively leverage the global financial system of capital markets, like small financial transfers, underregulated Islamic banking networks, and informal transfer systems throughout the world. They also have built a significant base of Islamic charities in Saudi Arabia with international divisions that have not been scrutinized or controlled by the regime, which in turn results in Al Qaeda's sophisticated financial network sustaining international efforts to disrupt it.

(c) Technologies and challenges to handle terrorism:

The growth of technologies has a large impact on the way terrorism is implemented. Technologies have been used for promoting as well as preventing terrorism. While terrorist groups used technology for recruitment, planning, communication, and attack, counter terrorism activities utilized it for threat detection, intelligence gathering, and response.

Bioterrorism is a part of using technology in terrorist activities, which creates panic and fear among the public. According to Rathish, Pillay, Wilson, et al. (2023), biological weapons are devices or agents deliberately used to disseminate disease using aerosol, food, water, or insect vectors. These biological agents can include bacteria, viruses, toxins, or fungi. Many specific biological weapons like Bacterial Agents (*Bacillus anthracis* (Anthrax), *Brucella* species (Brucellosis), *Burkholderia mallei* (glanders) and *Burkholderia pseudomallei* (melioidosis), *Franciscella tularensis* (tularemia), S*almonella typhi* (typhoid fever) and other *Salmonella* species (Salmonellosis), *Shigella* species (shigellosis) and *Escherichia coli* O157:H7, *Vibrio cholerae* (cholera), *Yersinia pestis* (plague)); Rickettsial Infections (*Coxiella burnetii* (Q fever), *Rickettsia prowazekii* (typhus fever), *Rickettsia rickettsii* (Rocky Mountain spotted fever), and *Chlamydia psittaci* (Psittacosis)); *Viral agents* (Variola Major (Smallpox), Viral Hemorrhagic Fevers, Viral Encephalitis); *Fungal Agents* (*Coccidiodes immitis* (coccidioidomycosis) and *Histoplasma capsulatum* (histoplasmosis); Protozoan Agents (Cryptosporidium parvum (Cryptosporidiosis)); *Toxins* (Ricin, Abrin, Botulinum Neurotoxins, *Clostridium Perfringens Toxins, Tetrodotoxin*); and Nerve Agents are the major ones as mentioned by Rathish, Pillay, Wilson et al (2023). Bioterrorism involves the deliberate release of bioweapons to cause death or disease in humans, animals, or plants. Certain properties of biological pathogens, like ease of procurement, simplicity of production in large quantities at minimal expense, ease of dissemination with low technology, and potential to overwhelm the medical system with large numbers of casualties, made it a favorite terrorism weapon. In addition to these, there are other advantages made these weapons as ideal terrorist weapons like silent dissemination of a biological agent and allowing the perpetrator to escape from the scene due to the incubation period (Venkatesh & Memish, 2003; Williams, Armstrong & Sizemore, 2023; Kortepeter, Cieslak, & Eitzen, 2001; Rathish, Pillay, Wilson et al.,2023). Kortepeter, Cieslak, & Eitzen (2001) reported that biological-weapons programs of the former Soviet Union and Iraq have heightened concern that countries with offensive-research programs.

Many suggestions and action plans were taken to prevent and tackle bioterrorism. The Biological Weapons Convention (BWC) is an international community's efforts to address bioterrorism, which effectively prohibits the development, production, acquisition, transfer, stockpiling, and use of biological and toxin weapons (UN). DaSilva (1999) suggested enactment of national laws that criminalize the production, stockpiling, transfer and use of chemo- and bioweapons and monitor the use of precursor chemicals that lend themselves to the development of chemical and bio-weapons, establishments of national and international databanks that monitor the traffic of precursor chemicals, their use in industry outreach programmes, and their licensed availability in national, regional and global markets. Also, the establishment and use of confirmatory protocols in the destruction and dispersal of outdated stockpiles, and chemical precursor components. He emphasized that adherence to the Biological and Toxin Weapons Convention reinforced by confidence-building measures sustained by the use of monitoring and verification protocols is indeed an important and necessary step.

Gronvall (2017) recommended that the US government should continue to support the Biological Weapons Convention strongly, should strengthen deterrence of biological weapons, to increase its support for private sector efforts to screen gene synthesis orders, to strengthen intelligence collection, to control legitimate science and to consider an educational and awareness-raising campaign should be part of scientific training.

Developments in the internet and social media have also influenced terrorism. According to Laura Mayer Lux (2018) the concept of cyberterrorism usually refers to a range of very different actions, from the simple spread of propaganda online to the alteration or destruction of information and even to the planning and carrying out of terrorist attacks via the use of computer networks and they specified that for cyberterrorism to exist, terrorist behavior must be perpetrated in cyberspace and for terrorist activities to be executed in cyberspace, the behavior carried out "in" or "through" cyberspace must have a structure, a harm principle, and the elements that allow it to be classified as such.

Low cost of connection to the network and state of art of technologies made it easy for terrorist to use it for multipurpose such as recruiting new followers, environment to indoctrinate and train the different members of a (cyber)terrorist organization, to spread propaganda, and to articulate financing strategies for (cyber)terrorist groups (Neubacher, 2014, Grabosky, 2009, Miro Llinares, 2012; Cohen, 2002). According to Lyon (2003), four main means of improving technological surveillance have been proposed since September 11th. They are: biometrics, the use of data extracted from the body, such as an iris scan, digital image, or fingerprint; identification (ID) cards with embedded programmable chips (`smart cards'); and enhanced software to detect facial recognition by CCTV and communication measures. Since the real dimensions and potential of cyberterrorism are not yet clear, reacting with preparation becomes difficult (Lux, 2018).

CONCLUSION

Literature on terrorism, counter terrorism measures, programmes and policies clearly pointed out many loop poles in this area and further suggestions. In a survey on the effectiveness of the preventive policies of terrorism, Haigner, Schneider &Wakolbinger (2012) checked the whether the effective tax information exchange would bolster AML/CFT policies especially on money laundering and terrorist financing and reported that such a strategy can reduce financial flows, yet due to a "weakest link problem" even a few countries not participating can greatly undo what others have achieved. After examining 550 pieces of scholarly literature covering both terrorist financing and global counterterrorist financing (CTF) to develop a typology of seven main approaches to CTF, Davis (2022) opinioned that there is little consensus on what these policy and practice have achieved, and little empirical evidence to determine if, or how, CTF works to reduce the financing of terrorism or terrorism more broadly. Poor articulation of the specific approaches and the overemphasis in the literature on criminalization of terrorist financing and the financial exclusion (sanctions) approach were the reasons for it, and she recommended considering different CTF approaches and evaluating these approaches individually to design better policies and practices. After examining the anti-money laundering measures and the activities of regulatory and professional bodies both domestically and internationally, Mei Leong (2007) reported that despite the enormous efforts and co-operation by the governments, law enforcement agencies, professional bodies and private financial institutions, money laundering and terrorist financing remain as threatening issues and also raised a concern that stricter regulation may add burden on the financial industry.

Many reports emphasized the importance of evidence-based research on counterterrorism strategies and criminal justice interventions. To identify existing evidence that considers the effectiveness of criminal justice interventions in preventing radicalisation, violent extremism and terrorism, Sydes et al (2023) reviewed literature related to criminal justice prevention from January 2002 to December 2021. Their systematic search identified 63,763 unique records, and 70 studies were eligible for the Evidence and Gap Map (EGM means the existing evidence and gaps in the evaluation research). The result showed that the majority of studies (n = 58) were on policing interventions, and limited evidence was found related to courts or corrections interventions, especially on effectiveness against measures of extremism and/or radicalisation. In a review of terrorism literature and counter-terrorism strategies, Lum, Kennedy & Sherley (2008) reported that almost complete absence of evaluation research on counter-terrorism strategies and concluded that counter-terrorism policy is not evidence-based and they emphasized the need for government leaders, policy makers, researchers, and funding agencies to be included in the committees and insisted for the evaluations of the effectiveness of these programs. As mentioned by Sydes et al (2023) conducting high-quality evaluation research on terrorism is rare, and significant gaps are found in studies evaluating criminal justice responses to terrorism and radicalisation. More hidden problems of terrorism present a challenge for criminal justice research, and they suggested sound measurement of terrorism-related outcomes to better capture the potential benefits and harms.

REFERENCE LIST

Angela Veng Mei Leong (2007). *The Disruption of International Organised Crime – An Analysis of Legal and Non-legal Strategies*. Hampshire: Ashgate Publishing Ltd. ISBN 139780754670667

Aninat, E., Daniel,D., Johnson,R.B. (2002). Combating Money Laundering and the Financing of Terrorism. *Finance and development*: F&D; a quarterly publication of The International Monetary Fund. Washington, DC: Fund, ISSN 0145-1707, ZDB-ID 20175. - Vol. 39.2002, 3, p. 44-47

Basile, M. (2004). Going to the Source: Why Al Qaeda's Financial Network Is Likely to Withstand the Current War on Terrorist Financing. *Studies in Conflict & Terrorism*, 27(3), 169–185. https://doi.org/10.1080/10576100490438237

Cohen, F.(2002). Terrorism and Cyberspace. *Network Security.* (5), 17-19. Recuperado de 10.1016/S1353-4858(02)05015-8 [Links]

DaSilva, E. J. (1999). Biological warfare, bioterrorism, biodefence and the biological and toxin weapons convention. *Electronic Journal of Biotechnology*, 2(3). Retrieved from https://www.ejbiotechnology.info/index.php/ejbiotechnology/article/view/v2n3-2

Davis, J. (2021). Prevention of Terrorist Financing. In *Handbook of terrorism prevention and preparedness*, 444-473. (Ed. Schmid, A.P) ICCT Press Publication. DOI: 10.19165/2020.6.01 ISSN: 2468-0486 ISBN: 978909033977

Davis, J. (2022). Understanding the Effects and Impacts of Counter-Terrorist Financing Policy and Practice. *Terrorism and Political Violence*, 36(1), 1–17. https://doi.org/10.1080/09546553.2022.2083507

Grabosky, P. (2009). International Handbook of Criminology. In Schneider, H (eds.); *High Tech Crime: Information and Communication Related Crime*. (73-101). Berlin: De Gruyter [Links]

Gronvall G. K. (2017). Prevention of the Development or Use of Biological Weapons. *Health security*, 15(1), 36–37. https://doi.org/10.1089/hs.2016.0096

Haigner, S.D., Schneider, F. and Wakolbinger, F. (2012). Combating money laundering and the financing of terrorism: A survey. *Economics of Security Working Paper* 65, Berlin: Economics of Security. Available from: https://www.researchgate.net/publication/254405916_Combating_Money_Laundering_and_the_Financing_of_Terrorism_A_Survey https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52001PC0521#:~:text=Terrorist%20offences%20can%20be%20defined,social%20structures%20of%20a%20country.

https://www.fbi.gov/stats-services/publications/terrorism-2002-2005#:~:text=Terrorism%20is%20defined%20in%20the,Section%200.85).

https://www.un.org/ruleoflaw/files/n0454282.pdf

https://www.unodc.org/e4j/en/terrorism/module-4/key-issues/defining-terrorism.html

Jean-Marc Sorel (2003). Some Questions About the Definition of Terrorism and the Fight Against Its Financing, *European Journal of International Law*, 14, 2, 365-378, https://doi.org/10.1093/ejil/14.2.365

Kortepeter, M. G., Cieslak, T. J., & Eitzen, E. M. (2001). *Bioterrorism. Journal of environmental health*, 63(6), 21–24.

Lum, C., Kennedy, L. W., & Sherley, A. (2008). Is counter-terrorism policy evidence-based? What works, what harms, and what is unknown. *Psicothema*, 20(1), 35–42.

Lux.L.M.(2018).Defining Cyberterrorism. *Revista Chilena De Derechom Tecnologia*, 7 (2), 5-25. Doi:10.5354/0719-2584.2018.51028 {7}

Lyon, D. (2003).Technology vs `Terrorism': Circuits of CitySurveillance since September 11th. *International Journal of Urban and Regional Research*, Volume 27, 3, 666-678.

Lyon, D. (2003).Technology vs `Terrorism': Circuits of CitySurveillance since September 11th. *International Journal of Urban and Regional Research*, Volume 27, 3, 666-678.

Miró Llinares, F. (2012). *El cibercrimen*. Madrid: Marcial Pons [Links]

National Research Council (US) Panel on Biological Issues. Countering Bioterrorism: The Role of Science and Technology. Washington (DC): National Academies Press (US); 2002. 3, Prevention, Response, and Recovery. Available from: https://www.ncbi.nlm.nih.gov/books/NBK221142/

Neubacher, F. (2014). *Kriminologie*. Baden-Baden: Nomos [Links]

Rathish B, Pillay R, Wilson A, et al. (2023). Comprehensive Review of Bioterrorism. [Updated 2023 Mar 27]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2025 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK570614/

Sydes, M., Hine, L., Higginson, A., McEwan, J., Dugan, L., & Mazerolle, L. (2023). Criminal justice interventions for preventing radicalisation, violent extremism and terrorism: An evidence and gap map. *Campbell systematic reviews*, 19(4), e1366. https://doi.org/10.1002/cl2.1366

UN. https://disarmament.unoda.org/biological-weapons/

United Nations Global Counter-Terrorism Strategy (General Assembly resolution 60/288, annex)

Venkatesh, S., & Memish, Z. A. (2003). Bioterrorism-a new challenge for public health. *International journal of antimicrobial agents*, 21(2), 200–206. https://doi.org/10.1016/s0924-8579(02)00366-7

Williams M, Armstrong L, Sizemore DC. (2023). Biologic, Chemical, and Radiation Terrorism Review. [Updated 2023 Aug 14]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2025 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK493217/

Milica Sekulović[1]
Aleksandra Bulatović[2]

JUVENILES AND ORGANIZED CRIME - SOCIAL AND HISTORICAL-PEDAGOGICAL PERSPECTIVES ON PREVENTION[3]

Abstract

The phenomenon of juvenile delinquency in contemporary society is increasingly associated with organized criminal groups, which use children as perpetrators of criminal acts due to their perception that they are less susceptible to detection and sanctions. This trend, which includes the role of juveniles in drug trafficking and money laundering, indicates the need for a comprehensive approach to prevention. The paper examines the phenomenon of juvenile delinquency through a historical-pedagogical framework, tracing the issue from the period of the Kingdom of Yugoslavia, through the socialist period, to contemporary challenges. Special emphasis is placed on the contribution of Anton Skala to the development of special pedagogy and his approach to the analysis of social factors that influence the formation of juvenile delinquents. Through a synthesis of pedagogical, social, and criminological perspectives, the text analyzes how historical approaches can contribute to contemporary preventive strategies, with the aim of a more efficient response to the problem of juvenile crime within organized criminal activities. The authors propose specific measures and social policies that can reduce the participation of juveniles in criminal groups and improve prevention in line with contemporary social challenges.

Keywords: *Juvenile Delinquency, Preventive Strategies, Historical-Pedagogical Experience, Prevention Strategies.*

INTRODUCTION

The connection between juvenile delinquency and organized crime has become one of the most serious challenges faced by modern social systems. Although delinquency – defined as the commission of criminal acts by young individuals – is not a new phenomenon, recent decades have witnessed significant changes in both the nature

[1] Institute for Philosophy and Social Theory, University of Belgrade, Serbia, milica.sekulovic@ifdt.bg.ac.rs

[2] Institute for Philosophy and Social Theory, University of Belgrade, Serbia

[3] This article was realized with the support of the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, according to the Agreement on the realization and financing of scientific research 451-03-136/2025-03/ 200025.

and scope of this issue, particularly in the context of increasing links between youth and organized criminal groups (see Alleyne&Wood, 2010; O'Brien et al., 2013; Mc Guire, Evans, Cane, 2021). Within this broader social context, organized crime – with its complex and often transnational characteristics – has proven to be highly effective in recruiting young people, a particularly vulnerable social group, for various illegal activities (Bulatović&Pavićević, 2021). Juveniles are often easier targets for criminal organizations due to their perceived inability to comprehend the serious consequences of their actions and their reduced legal accountability.

Juvenile delinquency, therefore, cannot be viewed in isolation, as it is always intertwined with broader social, economic, and cultural circumstances. On a global level – especially over the last four decades – organized crime has become a serious international problem, and the increasing use of new technologies, particularly the internet, has enabled criminal organizations to expand their youth recruitment networks and manipulate young people more effectively, exploiting their vulnerabilities, frustrations, and desire for acceptance within a community. In this context, the analysis of juvenile delinquency becomes indispensable for understanding organized crime, as it is evident that juveniles are often the "loaded guns" in the hands of criminal organizations.

Scholarly approaches addressing this issue examine various aspects of juvenile delinquency, including its causes, consequences, prevention, and rehabilitation (see Agnew, 2005). Particularly significant is the insight into the specific methods through which organized crime exploits vulnerable youth to achieve its goals. Organized crime organizations are using grooming tactics to coerce, manipulate, and force young children into criminality to pay off unwanted debts by targeting the most vulnerable young people in society (Bulatović&Hrnčić, 2018). This phenomenon has long-term effects on society – not only does it threaten community safety, but it also creates profound social issues that impact the delinquents themselves, their families, and the wider community. The consequences of juvenile delinquency, as manifested through ties to organized crime, often include lasting trauma, criminal records, and severe social stigma that leaves young people with diminished chances for reintegration into society. The issue of juvenile delinquency also serves as a foundation for broader debates on justice, punishment, rehabilitation, and social responsibility.

In contemporary societies – especially those in transition or post-conflict settings – the phenomenon of juvenile delinquency is further complicated by specific social, economic, and political circumstances. In many countries, high levels of poverty, weak education systems, and family problems have created fertile ground for the growth of criminal activities among youth, who, for various reasons, spiral into criminal behavior. When this is compounded by international criminal networks that recruit youth through sophisticated methods of manipulation, the seriousness and global scope of the problem become clear.

The connection between juvenile delinquency and organized crime is not accidental but deeply rooted in social, cultural, and economic structures. Juveniles, who are in the early stages of life and still in the process of forming their identity and values, are especially vulnerable to the influence of criminal groups that offer them false hopes of quick and easy wealth, status, and belonging. This phenomenon presents a serious challenge to modern social systems, which must determine how to identify and prevent such criminal activities and how to provide effective rehabilitation mechanisms for young people who have entered the world of organized crime.

Addressing this issue requires societies to develop a comprehensive approach that includes not only stricter legal regulations but also effective prevention through the educational system, social assistance, family and community support programs, and specialized rehabilitation centers. We can significantly reduce the number of young people entering organized crime through systemic change and long-term strategy and offer them opportunities for a better future.

In the context of post-socialist countries, especially in the former Yugoslavia, analyses of juvenile delinquency have historically evolved in line with the specific political, economic, and social circumstances. During the socialist period, the concept of juvenile rehabilitation focused on building a socialist character. This period is marked by the strengthening of professional criminological and sociological discourse, as well as a growing specialization in the field of juvenile delinquency research[4]. In contrast, contemporary post-socialist transitions have introduced new challenges, considering the weakening of institutions and the rise of economic and social inequalities. Today, in post-conflict and post-transitional societies, the issue of juvenile delinquency is often central to political and social debates about how to respond to complex social problems while preserving the rule of law and human rights.

This issue is also closely linked to the broader global phenomenon of transitional justice and the pursuit of accountability for social injustices, while simultaneously developing effective mechanisms for youth reintegration. The phenomenon of juvenile delinquency and its connection to organized crime has thus become not only a local problem but a global challenge requiring joint action by states, international organizations, and civil society.

[4] Representatives of the Federal Secretariat for Public Health (SIV) organized a federal seminar on the problems of neglected children and juvenile offenders in Belgrade from March 21 to 30, 1955. The Proceedings from this seminar were intended to serve as a handbook for practical solutions to the problem of youth educational neglect. The initiative for the seminar came from the Council for Public Health and Social Policy of the People's Republic of Croatia, which, by its act 21.123-II-3-54, sent a proposal to all Republican councils in the country and the Federal Secretariat for Public Health and Social Welfare (Proceedings, 1955: 5).

This paper will examine the historical aspects of juvenile delinquency, the role of organized crime in youth recruitment, the sociological factors enabling this phenomenon, as well as recommendations for the prevention and rehabilitation of young offenders. By analyzing different approaches and theories, the groundwork will be laid for understanding contemporary problems and proposing models that may contribute to the reduction of this serious social issue. Integrating past and present experiences in addressing this issue may provide a foundation for the development of contextually appropriate preventive strategies.

HISTORICAL CONTEXT AND PEDAGOGICAL FOUNDATIONS

Juvenile delinquency – particularly in the context of organized crime – has deep roots in the historical development of societies, and societal attitudes toward this phenomenon have evolved across different political and social regimes. In the Kingdom of Yugoslavia and during the socialist period, approaches to juveniles who committed delinquent acts were often shaped by the ideological and political needs of the time. Accordingly, the image of the juvenile delinquent has been shaped through the lens of societal values that were sought to be achieved, with variations primarily in the emphasis placed on the underlying causes of risky behavior – ranging from psychological and intimate to broader structural factors. In those periods, juvenile delinquency was frequently seen as the result of "individual errors" or a lack of proper education and socialization. The regimes recognized the importance of the younger generation in preserving societal stability and progress and thus sought to change youth behavior through educational and rehabilitative mechanisms.

However, systemic societal issues – such as poverty, political repression, and social injustice – remained underexplored and were often ignored. Although institutions and systems, especially in the socialist period, attempted to create educational frameworks to address delinquency, these approaches were not always successful in capturing the full complexity of the problem. For instance, the educational system was not always capable of addressing the socio-economic challenges young people faced. Additionally, many of these systems were unable to respond to the growing technological and societal changes that began to shape new forms of delinquency.

To gain a deeper understanding of juvenile delinquency, it is essential to consider the political context in which these approaches developed. In socialist Yugoslavia, for example, the ideology of the socialist system often influenced how youth were treated. Despite notable efforts within social and educational spheres aimed at preventing juvenile delinquency, centralized governance structures proved insufficient in responding to wider societal challenges. This remained evident even following the introduction of school and pupil communities after 1958, which were intended to facilitate a more decentralized and democratic engagement with locally specific problems. Many social inequalities – such as poverty and the underdevelopment of rural areas – continued to pose high risks for youth, who became targets for organized criminal groups. Therefore, the historical context is not only helpful in understanding past approaches but is also crucial for shaping current policies regarding juvenile delinquency and organized crime. Past systems had certain positive initiatives, but also significant weaknesses that must now be taken into account when forming new strategies for prevention and rehabilitation.

The Kingdom of Yugoslavia: Pedagogical Foundations and Approaches to Juvenile Delinquency

During the period of the Kingdom of Yugoslavia, the societal response to juvenile delinquency was highly restrictive, yet there was a certain level of attention given to the education and social rehabilitation of young offenders. Through the court system and state institutions, juveniles were often treated as delinquents who, despite their age, were considered responsible and aware that their criminal acts could also be seen as the result of adverse social circumstances, such as poverty, neglect, or poor upbringing. Skala was among the pioneers in highlighting the preventive potential of educational influence on children at risk, critically observing the limitations of relying solely on punitive measures and incarceration (Skala, 1934). Although his approach to childhood retained essentialist elements, he paid close attention to the lived experiences and self-reflections of juvenile offenders, which provided insights into the social and personal circumstances leading to delinquent behavior. While his account lacks a fully developed scientific framework, Skala nonetheless emphasized the importance of creating an environment that would simulate a structured and meaningful life within the broader community.

The criminological approach during this period was based on the idea of social rehabilitation, though it lacked deeper analysis of the causes that led to delinquency. The emphasis was placed on punishment, while the educational system aimed to instill state norms in young people. This period was marked by high centralization and strong state control over all segments of society, including the educational system. Although there was a desire to ensure social security and stability, juvenile delinquency was often perceived as a threat to national security.

Socialist Yugoslavia: Focus on Education and Rehabilitation

The socialist period brought significant changes in the approach to juvenile delinquency, as the state recognized the need for preventive, rather than solely repressive, measures. During this time, rehabilitation became a central component of social policy toward juveniles, though there remained a strong emphasis on the socialist value system, which included ideals such as collectivism, work discipline, and loyalty to state ideology.

Pedagogy during this period, influenced by the socialist system, aimed to create the "new socialist man" through the educational system, while juvenile delinquency was viewed as a form of deviance from social norms. The state developed specialized institutions for juvenile delinquents, designed to rehabilitate youth through labor, education, and upbringing in the spirit of socialism. Rehabilitation efforts were embedded in an educational process firmly rooted in ideological instruction, though a prevention policy also emerged, encompassing educational reforms and social assistance.

A significant contributor to the development of pedagogical theory in socialist Yugoslavia was Antun Skala, one of the most prominent pedagogues of the time. Skala was a pioneer in special education, and his work on juvenile delinquency and theories of youth rehabilitation was instrumental in shaping educational systems dealing with these issues. He emphasized that youth delinquency was not merely a result of individual "deviations" but also of social factors such as family environment, education, and social status. His pedagogical theories, grounded in the concept of social prevention and rehabilitation, remain fundamental to analyses of juvenile delinquency in the former Yugoslavia. Skala believed that only through changes in social conditions and the educational system, along with community engagement, could juvenile delinquency be prevented and the foundation laid for the positive reintegration of young people into society.

Post-Socialist Transition: New Challenges and Issues in Approaching Juveniles

The collapse of socialism and the disintegration of Yugoslavia brought drastic changes to all aspects of social life, including approaches to juvenile delinquency. The post-socialist transition created a new social dynamic in which economic instability, rising poverty, unemployment, and a weakened social system became key factors shaping juvenile delinquency. The legal framework inherited from socialism lacked the flexibility needed to address these new challenges, prompting many post-socialist countries – including the former Yugoslav republics – to introduce new strategies.

During the post-socialist period, the educational system faced new challenges: declining quality of education, reduced resources, and diminishing public trust in institutions. Pedagogical theories were largely marginalized, and the rehabilitation and resocialization of juveniles were often neglected due to a lack of adequate funding and professional personnel. In this context, organized crime became a serious issue, as criminal groups began to exploit the weaknesses of the system to recruit youth, particularly those growing up in adverse social and economic conditions.

This period was marked by an increase in the number of young people becoming members of organized criminal groups, which led to a new understanding and acknowledgment of juvenile delinquency. In many post-socialist countries, rehabilitation and prevention efforts were aimed at the political and social reintegration of youth, but pedagogical and social factors that enabled juveniles to enter criminal networks were frequently overlooked.

Historical Perspective and Contemporary Challenges

By analyzing the historical development of approaches to juvenile delinquency and organized crime across different political and social systems, we can gain a deeper understanding of the current challenges we face. Although pedagogical theories and social policies have evolved, the common challenge remains to address the root causes that lead to delinquency – particularly in the context of social factors and organized crime. Contemporary approaches must recognize the importance of prevention and rehabilitation while simultaneously offering concrete responses to global challenges related to modern organized crime and its impact on young people. The historical perspective provides essential lessons that can contribute to the improved implementation of prevention, protection, and rehabilitation strategies – not only through theoretical frameworks but also through concrete measures that can positively influence the reduction of juvenile delinquency in contemporary society.

Social Factors:
Poverty, Family Dysfunction, and Education

One of the most significant factors influencing juvenile delinquency is poverty. Children and adolescents growing up in impoverished environments often lack access to adequate education, healthcare, and other resources that can help them develop within a healthy and stable setting. Poverty creates conditions in which young people are more susceptible to substance abuse – such as drugs and alcohol – which further pulls them into criminal behavior. Moreover, youth growing up in poverty may become frustrated and lose hope for a better future, increasing the likelihood that they will seek out quick solutions through illegal activities.

Family dysfunction is another critical factor. In situations involving parental neglect, abuse, or alcoholism, young people often lack stable emotional support to help them cope with stress and social pressures. In such families, children are more prone to developing problematic behaviors, including delinquency. In some cases, these youth may seek out support in communities that provide an alternative sense of belonging – often through criminal groups that offer a sense of identity, protection, and material gain.

The educational system is also an essential part of any prevention strategy. Many young people who struggle to fit into formal educational frameworks may feel excluded and neglected, increasing the risk of engaging in criminal behavior. Inadequate education systems, substandard instruction, and widespread student disengagement often foster environments in which young people perceive no viable paths to secure their livelihoods, rendering them increasingly susceptible to recruitment by criminal networks.

THE IMPACT OF ORGANIZED CRIME ON YOUTH RECRUITMENT

Organized crime plays a major role in recruiting young people, particularly in marginalized communities struggling with poverty. Many organized criminals recognize the vulnerability of youth exposed to social exclusion and economic uncertainty and use these circumstances to attract them into their ranks. Organized criminal groups often offer youth easy access to income through activities such as drug trafficking, theft, extortion, and other criminal behaviors. For young people with limited options, crime may appear to be the only chance to improve their lives – at least in the short term.

The initial phase of youth recruitment into organized crime is often disguised as an act of "friendship" or "support." Many members of organized crime pose as mentors or role models, offering material security and social support that young people lack in their family or community environments. Unfortunately, over time, these young people become increasingly involved in criminal activities and lose the ability to distance themselves from criminal networks, leading to more serious and dangerous offenses.

One of the key factors facilitating the recruitment of youth into organized criminal groups is the perception of immunity from prosecution. Legal frameworks protecting juveniles in many countries, including Serbia, often provide a kind of immunity from criminal liability, as penalties are generally lighter than those for adults, and younger minors are not criminally responsible at all. Organized crime is well aware of these legal “loopholes” and exploits them by creating networks involving minors who can commit criminal acts without fear of severe consequences.

Globalization and Technological Advancement: New Challenges in Prevention

With globalization and advances in technology, organized crime has become more sophisticated, creating additional challenges in the prevention of juvenile delinquency. Today, young people have access to the internet, social media, and digital platforms that can be used to communicate with criminal groups – even without direct physical contact. Cybercrime, including online fraud, human trafficking, and internet drug trade, enables organized criminal groups to recruit young people in new and innovative ways. These activities are often difficult to detect, complicating further efforts to prevent and control these phenomena.

Technological advancements also enable greater mobility and faster information exchange among members of criminal networks, making them even more efficient. For youth already facing social and economic hardships, online criminal networks often appear as an easy escape from daily struggles, offering excitement and financial gain.

The Influence of Media and Popular Culture on Perceptions of Crime

Another important social factor shaping youth perceptions of delinquency is the influence of media and popular culture. Films, television shows, video games, and music often depict criminal activities in a way that makes them appear attractive and glamorous. Many young people – particularly those without stable social and emotional foundations – may identify with characters who live in a world of crime, which increases the likelihood that they will execute similar behaviors in real life. The media often exaggerate and romanticize criminal figures, creating negative role models for youth, especially in times when societal structures are weak and young people are searching for ways to express themselves or escape their problems.

The Complex Impact of Social Factors and Organized Crime

Social factors play a decisive role in shaping youth behavior and their involvement in organized crime. While individual traits – such as personality and family dynamics – do influence juvenile decisions, broader societal factors often provide the conditions that facilitate youth entry into the world of crime. Poverty, unemployment, social exclusion, and lack of educational opportunities are just some of the factors that allow organized crime to thrive in recruiting young people (see Sharkey, Besbris, Friedeson, 2017).

Social exclusion is one of the most significant contributors to why young people often turn to criminal groups for solutions to their life challenges. When youth lack access to quality education, employment, and other social resources, their connection to lawful social norms weakens. In such contexts, organized crime becomes an alternative that offers a sense of belonging, power, and security – something they cannot find in traditional structures such as schools, families, or workplaces.

Additionally, the absence of role models and appropriate behavioral examples may leave young people without a clear understanding of what constitutes acceptable behavior. Many grow up in communities where values such as violence, crime, or disregard for the law are part of everyday life. In these circumstances, organized criminal groups offer young men “quick” solutions to their needs for status, money, and recognition – especially when they feel that society does not offer real opportunities for personal advancement.

Family problems – such as abuse, neglect, or dysfunctional relationships – also play a key role in motivating young people to engage in criminal activities. Many juveniles from families struggling with mental health issues, addiction, or violence do not develop healthy emotional and social skills. These young individuals often seek escape from their problems in non-institutional groups that offer them “family-like” support. Criminal organizations frequently recognize this vulnerability and exploit it to recruit youth, creating an atmosphere of loyalty and protection that appears to offer an escape from their real-life struggles.

Social inequalities – particularly in societies with large economic disparities – can create ideal conditions for the spread of organized crime. Young people who grow up in poverty, with limited access to education and employment, often feel discouraged and hopeless. In such situations, criminal groups offering money, power, and social status become extremely appealing. Those most vulnerable are often youth lacking social networks or support outside their immediate surroundings, as they frequently find themselves with nothing to lose. As social and economic inequality increases, organized crime is more likely to expand in poor and marginalized communities.

Contemporary Approaches to Juvenile Delinquency Must Address Complex Social Factors

Modern strategies must operate on multiple levels. Prevention cannot focus solely on individual cases – it must address broader social conditions. Prevention programs that focus on improving education, reducing unemployment, supporting families, and developing social networks can play a crucial role in decreasing the likelihood that young people will become involved in organized crime.

Governmental and non-governmental organizations also play a vital role in reducing social inequalities and preventing juvenile delinquency. They should develop long-term strategies for social inclusion. This includes creating programs that offer educational and employment opportunities to youth from marginalized communities, as well as developing social services that support families. Additionally, joint initiatives involving government bodies, local communities, educational institutions, and the private sector can contribute to reducing poverty and improving social protection.

Understanding the social factors that enable juveniles to become involved in organized crime is essential for developing effective prevention and intervention strategies. These strategies must address the root causes of poverty, unemployment, social exclusion, and inequality, thereby reducing the risk of youth involvement in criminal activities and providing the foundation for healthier and more constructive development.

Contemporary Challenges and Preventive Strategies

Modern society is facing new challenges in combating juvenile delinquency as the dynamics of crime continuously evolve under the influence of globalization, technological progress, and social change. Organized crime is becoming increasingly sophisticated, and young people are more frequently involved in illegal activities through digital platforms. Recognizing and confronting the emerging challenges in this context is essential for developing effective preventive strategies. This section discusses how contemporary challenges impact the prevention of juvenile delinquency and which strategies may be effective in reducing the number of youth involved in criminal behavior.

Globalization and Digitalization: New Frontiers for Criminal Activity

One of the most significant contemporary challenges in the area of juvenile delinquency is globalization and digitalization. With the development of the internet and mobile technologies, organized crime has become more dynamic and more accessible to young people. Many criminal groups now use digital platforms such as social networks, forums, encrypted communications, and the dark web for recruitment, drug trafficking, human trafficking, and other criminal activities. These networks often provide anonymity and are difficult to trace, making the work of police and other authorities in combating crime significantly harder.

For young people growing up in a digital environment, recognizing the dangers associated with cybercrime can be extremely difficult, as many perceive the digital world as a safe space. Additionally, these technologies often facilitate easier involvement in criminal behavior by enabling hidden communication and global trade, which makes tracking criminals and their activities nearly impossible.

The Rise of Violence and the Pervasiveness of Danger

Another significant challenge in contemporary society is the rise of violence among youth. Violence in schools, in families, and within communities is becoming increasingly common and often acts as a factor encouraging young people to join criminal groups. Many young people exposed to violence at home or at school – and lacking appropriate mechanisms to cope with these challenges – often seek refuge in communities that provide a sense of support, which are frequently criminal groups offering protection and status.

These situations often result in the formation of new generations of juvenile offenders who continue the cycle of violence and criminal activity. Moreover, societies faced with such problems are often not adequately equipped to provide the necessary support and resources to deal with violence and its consequences, which only increases the likelihood that youth will fall into the trap of organized crime. identification of at-risk youth and timely intervention is viewed as a preventive strategy. The dichotomy between preventive and retroactive measures presents a substantive conceptual and practical challenge.

MODERN APPROACHES TO JUVENILE DELINQUENCY PREVENTION

To address the contemporary challenges associated with juvenile delinquency, it is necessary to develop a comprehensive prevention approach that is not based solely on repression but also on education, rehabilitation, and social support. Prevention must be integrated into social, educational, legal, and healthcare policies. The following are key approaches and strategies that may prove effective in reducing juvenile delinquency:

Education and Youth Inclusion

One of the fundamental aspects of prevention is the education of youth and the creation of an inclusive educational system that offers equal opportunities for all. Education is not merely a means of acquiring academic knowledge but also of developing social and emotional skills that help young people cope with stress, aggression, and social pressures. Schools should play a key role in prevention – not only through formal instruction but also through courses that strengthen emotional intelligence, social responsibility, and conflict resolution skills.

Family Support and Mentorship

Support for families, as well as the development of mentorship programs, can have a significant impact on prevention. Family dysfunction is one of the key factors contributing to problematic behavior among youth, so it is crucial to support parents and guardians through educational programs, therapy, and group support. In addition, mentorship from responsible adults who serve as positive role models can be highly effective in prevention, as it provides youth with behavioral models based on values, responsibility, and social integration.

Community Engagement and Prevention of Social Exclusion

Young people should be actively engaged in their communities through various social, sports, cultural, and volunteer activities. Connecting youth to their communities helps them develop a sense of belonging and identity, which reduces the likelihood that they will seek alternatives in criminal groups. Programs that involve youth in social projects, sports, and artistic initiatives can offer them opportunities for positive expression and help them develop interpersonal skills essential for future social adaptation.

Legal Framework and Institutional Responsibility

The legal framework must continually adapt to new social challenges. Although legislative changes may be slow, it is important to reform how the law treats juveniles, including expanding accountability for involving minors in organized crime. Special attention must also be given to building institutional capacity for effective law enforcement and to training police officers, social workers, and judicial bodies to work with minors. Institutions that deal with juveniles must collaborate to develop a coherent strategy that integrates legal, social, and educational systems.

Psychosocial Support and Rehabilitation

When young people are already involved in criminal behavior, rehabilitation becomes a key aspect of their reintegration into society. Programs that offer psychosocial support – including therapy, rehabilitative work activities, and group support – can help youth recognize the negative consequences of their actions and develop positive strategies for the future. Working with psychologists, therapists, and specialized counselors can play a vital role in their rehabilitation.

A Holistic Approach to Combating Juvenile Delinquency

Contemporary challenges related to juvenile delinquency require a comprehensive and multidimensional approach. Social, technological, and economic factors play key roles in shaping the behavior of young people, making it crucial to develop preventive strategies that integrate education, family support, social inclusion, and legal accountability. Effective prevention of juvenile delinquency must focus on strengthening young people’s social resilience, creating positive role models, and enabling the reintegration of those already involved in criminal activities.

CONCLUSION

The issue of juvenile delinquency – particularly when connected to organized crime – represents a complex social phenomenon that demands careful examination and a comprehensive approach. Understanding the causes of this phenomenon through historical, pedagogical, and social contexts not only offers valuable insight into how this issue has developed over time but also enables us to better comprehend the contemporary challenges we face. Through the analysis of both past and present factors shaping juvenile behavior, it becomes clear that only by integrating various approaches can we develop effective preventive and corrective strategies.

The historical context reveals that attitudes toward juvenile delinquency have shifted according to socio-political circumstances and ideological currents. The Kingdom of Yugoslavia and the socialist period were marked by specific approaches to young offenders, often motivated by a desire to "re-educate" and reintegrate them into society through work and education. While these approaches were aimed at rehabilitation, they sometimes failed to account for the broader social factors influencing youth behavior. The socialist period, although institutionally rich in its support for youth, often neglected the impact of social injustices and inequalities on their development.

Pedagogical approaches to juvenile delinquency – though developed through various theories and practices – have largely depended on the societal, political, and cultural conditions in which they were implemented. Pedagogy as a discipline has traditionally sought to understand the role of educational systems and institutions in shaping youth behavior, but it is increasingly turning toward the broader social factors that influence the individual. Historically, dominant approaches of the 20th century – including the work of special pedagogues like Skala – were grounded in the belief that youth delinquency stemmed from inadequate socialization, overly authoritarian educational systems, or, conversely, a complete lack of supportive educational and social structures.

Skala, for example, emphasized the importance of understanding the impact of social factors on youth behavior and developed theories that treated delinquency as a social phenomenon rather than a personal failure or misguided individual choice. In this context, juvenile delinquency was not seen merely as disobedience or misconduct but as a symptom of a broader social problem requiring multi-level intervention – through education, social protection, and collective community responsibility.

In today’s society, however, we are confronted with new challenges that cannot be resolved solely through pedagogical practices from previous decades. Although pedagogical insights developed by thinkers such as Skala often focused on individual approaches to delinquents, society now must embrace a much broader, holistic strategy.

Modern educational approaches, therefore, must take into account changes in the social environment, such as technological progress, evolving family structures, and globalization. For example, digital technology has become ubiquitous in the lives of young people, opening new avenues for delinquency – but also for prevention. Contemporary pedagogues must also address emotional and social education, as delinquent behavior often arises from emotional instability and underdeveloped social skills. This includes fostering social intelligence, emotional literacy, and conflict-resolution skills – all within preventive and rehabilitative programs.

In this regard, educational approaches can no longer be confined to theoretical educational models used in formal schooling. It is necessary to implement integrated strategies that involve working with families, understanding the dynamic nature of schools, the role of the community in shaping youth, and providing social and emotional resources through civil organizations. Furthermore, pedagogical work with youth must focus on building positive role models and mentorship so that at-risk youth feel supported rather than marginalized. For this reason, it is essential that pedagogy in the context of juvenile delinquency not remain static or rooted in outdated methods, but rather adapt to the realities of modern society. By working in partnership with communities, institutions, and experts from other fields – such as psychologists, sociologists, and social workers – educators can develop more effective strategies that not only respond to existing problems but also act preventively to reduce the number of young people entering the world of delinquency.

From the perspective of social factors, one of the key conclusions of this study is the limited effectiveness of institutional frameworks in addressing the pervasive social inequalities within the community. Many of the conditions that enable youth involvement in organized crime result from poverty, lack of educational opportunities, and family dysfunction. Social exclusion, absence of role models, inadequate education, and vulnerability to peer pressure lead young people to seek alternatives within criminal groups that often offer "quick" solutions to their needs for belonging, power, and status. Organized crime exploits these vulnerabilities and fosters a sense of legal immunity, creating a dynamic that facilitates youth integration into criminal organizations. This mechanism of creating perceived "immunity" from the law, through which organized criminal groups recruit youth, opens the door to the further development of delinquent behavior.

Contemporary challenges in combating juvenile delinquency are multifaceted. Globalization and technological advancement have enabled organized criminal groups to expand their operations beyond traditional boundaries, complicating the efforts of judicial and security institutions. The internet and digital technologies have made it easier for youth to access illegal activities such as drug trafficking, identity theft, and other forms of cybercrime. Consequently, legal and educational institutions face the challenge of responding rapidly to new forms of crime that are harder to detect and often fall outside the scope of existing legislation. Therefore, modern approaches cannot rely solely on traditional prevention methods; they must also involve understanding emerging phenomena and challenges, as well as developing new technologies and methods for prevention and suppression.

Preventive strategies, some of which have already been partially implemented, must become more comprehensive and adaptable, taking into account the specific challenges of contemporary society. This means revitalizing educational systems that not only provide academic knowledge but also focus on developing emotional and social competencies. Prevention must include training for parents to foster healthy family dynamics that deter delinquency and the creation of systems that view young people not just as offenders but as individuals with specific needs and potential for rehabilitation. Another key component of any preventive program should be support from social organizations working with youth in the community, engaging them in activities that promote inclusion and solidarity. Since organized criminal groups are often concentrated in socially and economically marginalized communities, preventive programs must target these areas with the support of social, governmental, and non-governmental organizations.

Combating juvenile delinquency connected to organized crime is a complex process that requires not only effective legal and judicial mechanisms but also deeply rooted preventive strategies based on an understanding of social factors, education and ongoing societal changes. Grasping the historical, social, and pedagogical context – combined with the implementation of modern preventive and rehabilitative models – holds the key to reducing levels of juvenile delinquency and organized crime. Through the integration of education, social protection, and prevention, it is possible to create a framework that offers young people opportunities for healthy and constructive development, thereby reducing their risk of exploitation by organized criminal structures.

REFERENCE LIST

Alleyne E. & Wood JL. (2010). Gang involvement: psychological and behavioral characteristics of gang members, peripheral youth, and nongang youth. *Aggressive Behaviour*, 36(6), 423-36.

Bulatović, A. & Pavićević, V. (2021). *Crna ekonomija i crno društvo*. Beograd: Institut za filozofiju i društvenu teoriju.

Bulatović, A. & Hrnčić, J. (2018). Juvenile Crime and Organized Crime Groups. In I. Stevanović (Eds.), *Pravda po meri deteta/Child Friendly Justice* (pp. 309-321). Institute for Criminological and Sociological Research.

McGuire, J., Evans, E., Kane, E. (2021). P*reventing Young People from Involvement in Violence, Gangs and Organized Crime*. Springer, Cham. https://doi.org/10.1007/978-3-030-76363-3_6

O'Brien et al. (2013). Youth gang affiliation, violence, and criminal activities: a review of motivational, risk, and protective factors. *Agression and Violent Behavior*, 18(4), 417-425.

Skala, A. (1934). *Zavodi za vaspitanje dece i mlađih maloletnika: sa gledišta savremene kriminalne pedagogike.* Beograd: Dom maloletnika.

Sharkey, P., M. Besbris, M. Friedson (2017). Poverty and Crime. In D. Brady, L. M. Burton (Eds.), *The Oxford Handbook of the Social Science of Poverty*, Oxford Handbooks (2016); online edn, Oxford Academic, 5 Apr. 2017), https://doi.org/10.1093/oxfordhb/9780199914050.013.28.

Zbornik materijala sa saveznog seminara o vaspitno-zapuštenoj deci i omladini (1955). Beograd: Komos.

***Kedeibaeva Zhamal Arstanalyevna*[1]**
***Bakhramzhanova Nilufar Mahamadjanovna*[2]**
***Shermatova Aizhanyl Mitaevna*[3]**

SOCIO-PHILOSOPHICAL ASPECTS OF THE PROBLEM OF NATIONAL AND SPIRITUAL SECURITY

Abstract

The problem of ensuring national security acquires almost dramatic significance in modern conditions for our country. Cardinal geopolitical changes in the last decade have radically transformed the organization of international relations established after the Second World War. These changes have significantly impacted the development of human civilization. Today, the dominant global power seeks to determine its position and role in the world.

Keywords*: State, Resources, Decisions, Security, People, Country.*

The conditions for our country's existence and development have fundamentally changed. Consequently, the threats we face have evolved, altering the tasks of their detection, prevention, and countermeasures. The tasks of providing our country with conditions of safe existence and development on the scale of the planet, taken in interrelation and interdependence with the internal situation in the state, with the problems and opportunities arising in it, imperatives and resources for their solution, and form the fundamental real state task, the continuous solution of which by the state and expressed directly in everyday life (including political life) by the concept of national security.

The problem of ensuring national security is gaining almost dramatic significance in modern conditions for our country. Cardinal geopolitical changes in the last decade have radically transformed the organization of international relations established after the Second World War. These changes have significantly impacted the development of human civilization. Today, the dominant global power seeks to determine its position and role in the world.

The rapid improvement of information technology, the aggravation of the environmental threat, other problems, and the development of the modern world give rise to new types of dangers and threats and, therefore, the need to develop strategic measures to prevent them. The identification of rational grounds for safe development, in society is

[1] Institute of Economics and Management, Osh Technological University, kedeybaeva1976@mail.ru

[2] Department of Business Management and Social Work, Institute of Economics and Management, Osh Technological University, Kyrgyz Republic

[3] Department Computational Linguistics, Industrial-pedagogical Institute, Osh Technological University

associated with establishing the optimal functioning of all spheres of public life, as well as a parity creation of security conditions for all categories of the population. Unfortunately, in modern Kyrgyzstan, there are real threats to destabilizing public life associated with various types of dangers, including global ones. Socio-philosophical analysis of the grounds for the safe development of society creates the possibility of theoretical substantiation and practical embodiment of such measures that allow the maximum to avoid the negative impact of the external environment. Of course, the solution to this issue depends not only on the creation of the concept of security but also on the scientifically based state and regional security policy. Such a policy requires the development of the methodological foundations of its formation, implementation, and increase in efficiency. Socio-philosophical analysis of the concept of security is an obligatory component of creating a comprehensive concept of security and its practical embodiment.

For all socially, and nationally thinking people of the country, the task of scientific development and philosophical understanding of the problem of personality and public security, civil and state security, personal and civil security, and public and state security, included in the concept of "national security" without any understanding of its attitude to the term "safeness", was acutely relevant.

In a comprehensive understanding of such a complicated phenomenon as national security, a fundamental philosophical approach, based on its world classics, cannot be required.

This is understandable at least from the fact that national security is correlated and closely interacts with the national consciousness. The content of national consciousness is the expression of the real conditions of its existence, including the practice of communicating with other people and the degree of use of their historical experience, as well as civilized norms of international relations and possible deviations from these norms. It is understandable that the idea of ensuring national security, to materialize, should go through national consciousness. It should be realized as a practical task, as an imperative of national life.

It is impossible to ignore the fact that each national community is socially heterogeneous, which gives rise to the corresponding heterogeneity of national consciousness. But, nevertheless, while the national community remains, in the national consciousness, the spiritual scrapers ultimately prevail, which ensure the contradictory integrity and dynamic stability of this nation.

Thus, thanks to its mobilization capabilities, national consciousness, as an adequate expression of national interest, becomes the most important factor in national security. And this is nothing more than a manifestation of the dialectics of national being and national consciousness.

All this of the above makes us turn to the problem of national security today. For it, our national security is under an increasing threat every year.

In recent years, a significant number of works have appeared in the literature, the authors of which explore certain aspects of spirituality, and consider it from different angles of vision. Among them are works devoted to the study of the essence of the spiritual and various aspects of its manifestation and functioning in the life of personality and society, as well as the conditions and factors of the formation and development of the spiritual world of a person. In them, along with the analysis of the main issue, certain aspects of knowledge about society and man are considered.

It can be argued that to date, scientists have achieved certain results in the study of the fundamental foundations of spirituality, the development of its categorical apparatus from the standpoint of modern domestic and world science, the creation of a unified concept of spiritual, in the study of its place and role in the system of spiritual processes taking place in the country and the world as a whole.

Currently, the "liberal" security model is being implemented in Kyrgyzstan.

In the concept of national security of the Kyrgyz Republic, approved by Decree of the President of the Kyrgyz Republic of July 13, 2001 No. 221, the national security is defined as "the creation and ensuring conditions for the life of the individual, society and the state and their protection from the influence of external and internal threats" [195, p. 308]. Such understanding of security is generally true, in the sense that the security of all individuals is a condition for the protection of each person and vice versa, that, without protecting society as a whole, it is impossible to protect individual individuals, and in a civilized society the defender of the society itself and those who make up it, i.e. persons, the state acts, therefore, without protecting the state, it is impossible to protect both society and the personalities forming its citizens who are citizens of this state.

A weak theoretical study of security issues is reflected in the fact that there is still debate about the possibility of using the phrase "national security". The term "national security" is tracing paper from the English words "National security", which, due to the identification of the Americans with citizenship, can be translated both as national and state security. But when distinguishing between citizenship and nationality, it is unacceptable to replace national security and vice versa, since we are talking about different objects allocated to the same people.

The foreign policy of states in all eras was decisively determined by what is now called national interest. Although the very concept of "national interest" has become a scientific circulation relatively recently.

What is national interest? What are its essence and parameters? How does it correlate with the concept of "state interest"? What is the relationship of national interest with national and spiritual security?

Often state interests are opposed by national and public (the interests of civil society). Often, recognizing their relationship, they still consider it advisable to determine them within the framework of the dichotomy "national interest - state interest";

“State interest is public interest”. However, such a contrast can be legitimate only for a situation when the state threatens the existence or even the normal development of the nation (people from many nations united and organized by one state.

As for state interest and public interest, they are also interconnected in the same way. State interest can withstand public interest only when the “state” destroys the “society”, when a certain state, as an organization and strength of a certain class. But in the ordinary life of societies, they represent them adequately before the rest of the world and only the state. Therefore, speaking of national interest, as a rule, they mean state interest and, conversely, state interest means national interest.

The interests of this nation (people from many nations united by one state), and this society of this nation (people) and this state arise, exist, and are specified by their geo-economic, geopolitical position and their resource capabilities at the points of crossing the many interconnected interests of the rest of the nations-state-states. Their formation has a powerful influence by the level of economic, political, and ideological development of the country (i.e. nation-state-state), its weight and place in the global economy, politics, and ideology of mankind.

Real national, social, and state interests affecting the sovereignty, integrity, and independence of their country are the main factors in the foreign policy activity of this state. As such, national interests are a fundamental historical phenomenon and cannot but exist as current factors, regardless of whether they are recognized by those nations whose interests they are or not. But the subject can be in the historical arena only the nation that is aware of its interests. Therefore, national interests have the closest relationship with the self-awareness of the nation from many nations), society, and (their) state, with the self-identification of this particular nation, this particular society, and this particular state.

In its extreme expression, national security in practice is a synonym for ensuring the survival of the state, because in the context of interstate relations, the survival of the people (nation) means the preservation of its national state as its total representative and organizer. National security is therefore closely related to the security of the state itself, the very guarantor of the security of the people living in this country. In the process of implementing their safety, the nation (people) deals with other nations not directly as a nation, but only through their state and in the name of their state with other states existing in other nations for the same reasons, with the same functions, and with the same goals.

Ultimately, all theorists of national security lead it out of what is called "national interest". However, the whole point is how to understand it. Here, absolutization is unacceptable as objectivity and the subjectivity of this phenomenon.

National security is, as has already been said, the security of an actual definite nation, of an actual definite people organized into a definite state. This nation can be a single nation, but it can also include a multitude of nations that make up the people (united into the people) of one state.

The national security of any country is determined by its historically established national interests.

National interest is one of the fundamental driving forces behind the behavior and activities of an individual, a community (nation), and society in general. National interests are present, one way or another, in all spheres of struggle and co-operation between people as representatives (individuals) of humanity. But they acquire the form of a legitimate institution, ultimately, only manifesting themselves in the structure and aspirations of certain states. A national community of people strives for the realization or even the exposition of its interests, for the consolidation of its success.

And, since there is no abundance of either land or other resources on the planet, important or even indispensable for the existence of people, this often comes at the expense of infringing on the interests of other nationalities, especially those in the minority. Conflicts between national interests arise, which are often resolved only through war, i.e. by the right of force.

National interests for any country are an objective factor conditioned by the totality of its historically developed vital needs and abilities, related to the conditions and means of its existence and development. Their content, which is different for each country, determines what the policy of the state should be, so that its integrity and survivability would be reliably ensured and protected, its citizens would live in a globally respected state, worthily representing and defending their interests in all corners of the planet.

The main objects of national security in all democratic States, including Kyrgyzstan, are: the individual - his or her rights and freedoms; society - material and spiritual values; and the State - its constitutional order, sovereignty and territorial integrity.

The main subject of ensuring national security is the state, which performs functions in this area through the legislative, executive and judicial authorities.

The subject and object of national security in general is and only the people who form a certain society. And society in modern conditions can be preserved and exist only by organizing itself into a state. Otherwise it cannot exist.

The attempt to focus on the interests of an abstract individual leads to an impracticable and very costly desire to create safe conditions for everyone, neglecting the security of the people and society as a whole. Behind the individual, the people with its historical individuality, destiny and interests are lost. The same applies to the question of society, which cannot be ‘society in general’, but our society, which ensures the historical existence of our people.

The object of national security in the state is considered by different specialists to be the existing social order protected by the state. It turns out that elements of the existing society not protected by the state do not fall under the object of national security.

An attempt to make the main object of national security the existing state system causes even more objections. Since he expresses society (representing one historical organism) even less than the existing social system. The old state system, which is absent in the changed conditions, is thus subject to change, and is thus put on the same level with the society itself. The recognition of the existing state system as the main object of national security pushes out not only the people but also the society formed by it. Although it is necessary to admit that there are situations, that it is to save themselves and their society that the people are forced to change their state system.

In order to preserve the state and the people, it is necessary to directly preserve its society, and for this, naturally, the personalities forming it, i.e. those representatives of the people.

It follows from the foregoing that the main and direct object of national and spiritual security is not a nation, but a society formed by it. If we destroy its society from the nation, it simply turns into a conglomerate of individuals who are not represented by a single whole, not united by a common spiritual life, ideas that are understandable to all and perceived, in fact, in the same way. As a result, such a scattered society turns into material for other societies and other nations, and may simply disappear physically, being torn from other societies and nations.

Although the subject of national and spiritual security ultimately is and can only be a nation (people), it cannot act as a direct subject of national security. If in the primitive era, each tribe was a society (community), and each society was formed (by the end of this era) from a certain tribe, then in a civilized society the situation is already completely different. Here the society alienated from individuals acts. And it can form both from one nation and from a certain set of nations that form the multinational people of this society. And in such a society, without a fatal for such a society, chauvinism and nationalism, cannot and should not talk about the greater protection of some nations and the smaller protection of other nations, now acting in the form of members of this particular society.

If national and spiritual security is considered through the prism of national interests, when national interests should be understood as a hierarchy of life-sustaining interests of society, then the main object of national and spiritual security is objectively society as a whole, society as a whole, society as a historical organism, society as a carrier of history and culture of a certain people. The national interests of a country, assessed through the historical interests of its people, have a long-term character and determine the main goals of national security policy, form the strategic and current tasks of the internal and external policy of the state as the main subject of this security and are implemented through the organization of state management of both society as a whole and individual individuals and communities that are part of this society and form this society.

An external condition for the implementation of national interests is the ability to independently solve internal political, economic, and ideological, as well as social problems, regardless of the intentions and positions of other states and their coalitions. Therefore, a clear, precise and definite position on the national interests of a country is the starting point in the formulation of the programme of action of any national government. Such a position underpins action.

National interests, both internal and external, cannot remain eternal and unchanging. As the objective reality changes inside and outside the country and the world, the content of national interests and the strategy of the state's activities to ensure these interests change. However, the fundamental external national interests that it is obliged to pursue, such as the preservation by its people of itself, the integrity of its life-supporting land, their historically obtained and created national wealth, and its culture, remain unchanged for the nation-state.

In addition, when realizing its own national interests, any State must take into account the national interests of other States, achieving a certain balance between them. Without this, it is impossible to maintain today and in the future the optimal level of international security for one's country, in which only the national interests of its people can be reliably ensured.

Specific internal and external threats to national and spiritual security presuppose a corresponding set of goals and objectives and ways to address them. Among the obvious internal prerequisites that ensure the national and spiritual security of our country, we should name in the first place:

- The unification of the people for the solution of national tasks of spiritual and material order, the awareness of its representatives of their own interests and the manifestation of an organized will to protect them;
- optimized state institutions that are ready to ensure the protection of national interests and guarantee the stable and harmonious development of society;
- advanced spiritual, cultural and scientific development;
- preservation of general stability in the state, prevention of our state's involvement in foreign warfare;
- establishing relations of business mutually beneficial partnership with all states of the world, but also taking into account the distant historical perspective;
- ensuring reliable defense of the sovereignty, integrity and security of our state;
- maximum possible expansion of integration processes in the commonwealth of post-Soviet countries;
- preserving the environment both within the country and throughout the Central Asian region, with the combined efforts of all other countries in the region;
- ensuring effective suppression of organized crime, elimination of criminal factors, and creation of guarantees for the personal security of citizens.

Obviously, not all of the above prerequisites are directly related to ensuring spiritual security, but without the creation of these prerequisites it is impossible to successfully solve problems related to ensuring spiritual security.

In conclusion, let us summarize the findings:

1. Each particular state and nation, due to a variety of reasons and conditions, has to solve its own set of problems related to ensuring both national and spiritual security. At the same time, significant differences between people and states in their economic, technological and military power, in the number of population leads to the fact that some people and states appear on the historical arena as a force capable and striving to impose their will, culture and language on other people, and others - as a party that must in one way or another perceive the influence and pressure. It is not only a question of economic and military pressure, but also of cultural and spiritual influence.
2. As history and long practice show, states and people, if favorable conditions exist, strive to expand their territories. In expanding their territories, it is necessary to spread their influence, including cultural and spiritual influence. The underlying motive for expansion is the obvious desire of human beings, specific people to extend their influence, power, domination over those who have less power and influence. This desire is ingrained in us by nature itself, i.e. it is an essential part of human nature, and it can be defined as the will to power, to dominate, which is ultimately the will to live.
3. Due to the presence of a person of the mind and its social nature, the phenomenon of will to power is embodied in much more complex and diverse forms than in the rest of the living nature, but the principle itself remains unshakable, maintaining its versatility. As all historical experience shows, people strictly and relentlessly and strictly followed and followed this principle, trying to spread their power everywhere where it is only possible. At the same time, culture acts as one of the necessary and important tools for the influence and spread of one's strength and influence, strong consolidation in foreign territories.
4. The process of competition between people and states practically began from the moment of their emergence, or rather, the competition between clans and tribes naturally transformed into the struggle of people and states as soon as they emerged. From the moment the first states and civilizations emerged, cultures were already so different from each other that conflicts and wars between states took the form of conflicts and wars between cultures and, consequently, between the spiritual phenomena that represented these cultures.

REFERENCE LIST

Abramov, Y.F. et al. (1998). *Information civilization: nature and prospects of development* [Text] / Y.F. Abramov et al. - Irkutsk: Editorial and Publishing Department of Irkutsk State University. p. 97.

Astakhova, L.V. (2010). *Information security: hermeneutic approach* [Text] / L.V. Astakhova - Moscow: RAN. p. 185.

Bell, D. (1999). *The Coming Postindustrial Society. Experience of social forecasting* [Text] / D. Bell - Moscow: Academia. p. 956.

Vozzhenikov, A.V. et al. (2000). *Main conceptual provisions of the national security of Russia in the XXI century* [Text] / A.V. Vozzhenikov - M.: EDASPAK. p. 48.

Dzliev, M.I. et al. (2001). *Problems of security: theoretical and methodological aspects* [Text] / M.I. Dzliev - M.: MGUK. p.192.

Zakharov, M.Y. (1995). *Security of the society as a philosophical and methodological problem* [Text] / M.Y. Zakharov - Monino. p.198.

General theory of national security. (2005). M.: RAGS [Electronic resource]. Access mode: http://www.iwolga.narod.ru/docs/bezop/otnb.sov

Spiritual security: conflicts on a worldview basis [Electronic resource]. Mode of access: http://credonew.ru/content/view/1243/68/.

Kuvaldin V.B. (2000). *Globalization bright future of mankind? On the threshold of the XXI century mega-society acquires real outlines* // NG-scenarios, October 11, 2000. [Electronic resource]. Access mode: http://scenario.ng.ru/interview/2000-10-1 l/5future.html.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

351.861(048)(0.034.4)
327.56:351.861(048)(0.034.4)

INTERNATIONAL Scientific Conference - BINS 2025 Transdisciplinarity of security studies and practice (2025 ; Belgrade)
Book of Abstracts [Електронски извор] / International Scientific Conference - BINS 2025 Transdisciplinarity of security studies and practice, Belgrade, May 8-9, 2025; [editor Milica Bošković]. - Belgrade : Faculty of Diplomacy and Security, 2025 (Belgrade : Faculty of Diplomacy and Security). - 1 електронски оптички диск (CD-ROM) : tekst ; 12 cm

Sistemski zahtevi: Nisu navedeni. - Tiraž 100.

ISBN 978-86-87545-49-6

а) Безбедност -- Међународни аспект -- Апстракти
б) Национална безбедност -- Апстракти
в) Безбедносни сектор -- Апстракти

COBISS.SR-ID 162889993

PROJECT PARTNERS:

FDB FACULTY OF DIPLOMACY AND SECURITY

UNIVERSITY OF TARTU

University of Tuzla
Bosnia and Herzegovina

УНИВЕРЗИТЕТ У БАЊОЈ ЛУЦИ
UNIVERSITY OF BANJA LUKA

УНИВЕРЗИТЕТ БИЈЕЉИНА
MMXII
BIJELJINA
UNIVERSITY BIJELJINA

UCG
University of Montenegro

Center for Social
Innovation

WEBIN
Western Balkans Institute