Original Scientific Paper/Original naučni rad UDC/UDK: 005.334:[004.8:623
Paper Submitted/Rad primljen:31.12.2025.
Paper Accepted/Rad prihvaćen:10.01.2026.
DOI: 10.5937/SJEM2601037J

Rizici i upravljanje autonomnim oružjem u savremenom ratovanju: Sveobuhvatna analiza

Katarina Janković[1], Milica Mladenović[2], Nenad Komazec[3]

[1] General Staff of the Serbian Army, Directorate for Development and Equipment J-5, Technical Test Centre, Centre for Testing Armaments and Military Equipment, Nikinci, Republic of Serbia, jankovickatarina95@gmail.com
[2] Regional Association for Security and Crisis Management RABEK, Belgrade, Serbia, mladenovicmilica21@yahoo.com
[3] Military Academy, University of Defence, Belgrade, Serbia, nenadkomazec@yahoo.com

Rezime: Brz tehnološki napredak u oblasti veštačke inteligencije (VI) menja savremene vojne sposobnosti i uvodi autonomno oružje kao važno strateško i etičko pitanje. U radu se analiziraju rizici koji prate uvođenje autonomnog oružja u savremene sukobe, kao i njegov tehnološki potencijal i bezbednosni izazovi. Razvoj i širenje autonomnog oružja predstavlja složenu tehnološku inovaciju koja prevazilazi uobičajene obrasce vojnog angažovanja. Napredne VI tehnologije menjaju međunarodne bezbednosne okvire i otvaraju etičke i operativne dileme bez presedana. U radu se sprovodi analiza rizika koja obuhvata tehnološke, geopolitičke, pravne i etičke aspekte primene autonomnog oružja. Metodologija istraživanja obuhvata proces identifikacije, procene i upravljanja rizicima. Kroz analizu relevantne literature, konsultacije sa ekspertima i modeliranje različitih scenarija, razmatraju se rizici poput algoritamske pristrasnosti, nenamerene eskalacije sukoba, izazova u određivanju odgovornosti i mogućnosti da sistemi deluju van ljudske kontrole. Rezultati pokazuju da autonomno oružje pruža određene taktičke prednosti, ali istovremeno stvara ozbiljne izazove za globalnu bezbednost. Nalazi ukazuju da međunarodna zajednica mora da razvije snažne mehanizme upravljanja i efikasne mere kontrole rizika. Završni deo rada predlaže okvir za smanjenje rizika koji podrazumeva saradnju stručnjaka za tehnologiju, donosioca odluka, vojnih planera i etičara. Ovakav pristup doprinosi aktuelnoj raspravi o odgovornoj primeni veštačke inteligencije u vojnim sistemima i naglašava potrebu za proaktivnim upravljanjem rizicima koje usklađuje tehnološke inovacije, etičke principe i zahteve globalne bezbednosti.

Keywords: Rizik, Upravljanje rizicima, Autnomno oružje, Veštačka inteligencija, Vojne tehnologije, Globalna bezbednost

Risks And Management of Autonomous Weapons In Contemporary Warfare: A Comprehensive Analysis

Abstract: The rapid technological advancement in artificial intelligence (AI) has precipitated a paradigm shift in military capabilities, with autonomous weapons emerging as a critical domain of strategic and ethical concern. This research critically examines the multifaceted risks associated with the integration of autonomous weapons systems into military conflict landscapes, exploring their technological potential and inherent security challenges. The proliferation of autonomous weapons represents a complex technological innovation that transcends traditional military engagement strategies. By leveraging advanced AI technologies, these systems challenge established international security frameworks and introduce unprecedented ethical and operational uncertainties. This study conducts a comprehensive risk analysis that encompasses technological, strategic, legal, and humanitarian dimensions of autonomous weapon deployment. The research methodology employs a systematic approach to risk identification, assessment, and management. Through comprehensive literature review, expert consultations, and scenario modelling, the study investigates potential risks such as algorithmic bias, unintended escalation, accountability challenges, and the potential for autonomous systems to operate beyond human control. The analysis reveals that while autonomous weapons offer significant tactical advantages, they simultaneously introduce substantial risks to global security architectures. Key findings underscore the critical need for robust international governance mechanisms and comprehensive risk management strategies. The research proposes a multi-stakeholder framework for mitigating autonomous weapon risks, emphasizing the importance of

interdisciplinary collaboration among technologists, policymakers, military strategists, and ethicists. By providing a nuanced understanding of autonomous weapon risks, this study contributes to the emerging discourse on responsible AI development in military contexts. The findings advocate for proactive risk management approaches that balance technological innovation with ethical considerations and global security imperatives.

Keywords: Risk, Risk Management, Autonomous Weapons, Artificial Intelligence, Military Technology, Global Security

1. Introduction

The rapid development of artificial intelligence is transforming the way modern armed forces plan, decide, and conduct military operations. This process introduces a new generation of combat systems in which autonomous weapons hold a central position. Autonomous systems provide a high level of automation, fast reaction times, and the ability to operate in dynamic environments, while simultaneously creating significant security, ethical, and geopolitical challenges. Contemporary armed conflicts demonstrate the growing use of algorithmically supported systems that identify targets, make decisions, and execute tasks with minimal or no human supervision. Examples from recent conflicts show that artificial intelligence accelerates combat activities but also increases the risk of unintended escalation and target misidentification (Jankovic, Mladenovic & Komazec, 2025). Autonomous weapons thus become a source of tactical advantage, as well as a potential cause of consequences that are difficult to predict and control.

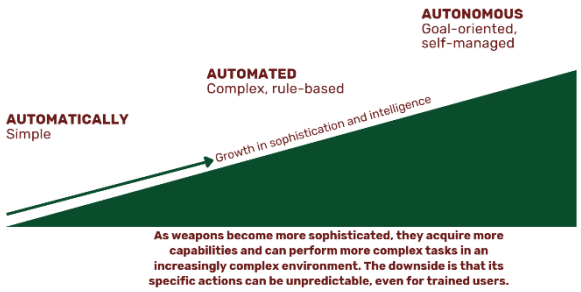
The risks associated with these systems extend beyond traditional military frameworks. Algorithmic bias, errors in pattern recognition, cyber intrusions, and loss of control can lead to incidents with serious consequences for military units, civilian populations, and international stability. The issue of accountability becomes particularly prominent when autonomous systems make decisions faster than humans can intervene.

In such an environment, the need for a systematic approach to managing the risks of autonomous weapons continues to grow. An analysis of technological, legal, geopolitical, and ethical factors enables a clearer understanding of the capabilities and limitations of these systems. The development of risk-management models provides the foundation for their responsible, controlled, and safe use. The aim of the paper is to offer a comprehensive overview of the risks posed by autonomous weapons and to propose a framework for their responsible application in modern warfare.

2. Characteristics of Autonomous Weapons

Modern weapons systems are undergoing significant technological transformation, and the development of autonomous weapons represents one of the fastest-growing innovations. Although the term autonomous weapons is often used as if it has a clear definition, in practice it involves considerable ambiguity. The greatest confusion arises from the distinctions between automatic, automated, and autonomous weapons, which complicates the understanding of this new generation of systems based on artificial intelligence (Figure 1).

Figure 1: Automatic, automated and autonomous weapons



Source: (Scharee, 2020)

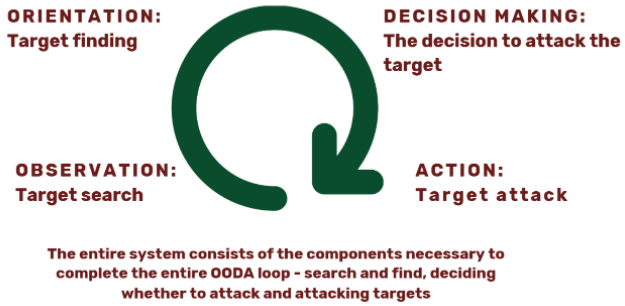
To understand what autonomous weapons represent, it is necessary to distinguish between the basic terms used for modern weapons systems (Janković, Komazec & Erkic, 2023). Three concepts appear in current use—automatic, automated, and autonomous weapons—and the boundaries between them are often fluid because these technologies overlap.

Automatic systems operate in a simple manner and do not include any decision-making process. They react only to the physical act of pulling the trigger and rely on basic mechanical principles. Automated systems represent a more advanced level: they process a greater volume of input data, combine multiple variables, and select a response based on predefined rules.

Autonomous weapons stand above these two levels. They use artificial intelligence algorithms that enable the system to perform tasks independently, such as sensing, locating targets, selecting targets, and executing attacks (Scharee, 2020) (Figure 2). This level of capability surpasses classical automation and introduces decision-making with or without direct human supervision.

Autonomy refers to the ability of a machine to perform a task independently. Although there is no internationally agreed definition of autonomous weapons, one of the definitions used in the working groups of the International Committee of the Red Cross states: „Autonomous weapon systems are weapons that can select and attack targets independently of human intervention, that is, with autonomy in their 'critical functions' of acquiring, tracking, selecting, and attacking targets" (International Committee of the Red Cross, 2014).

Figure 2: Components of Autonomous Weapons



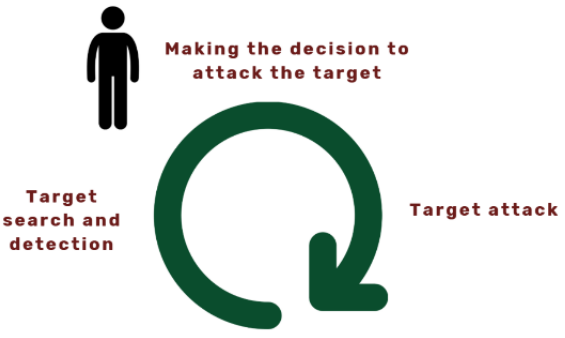
Source: (Scharee, 2020)

Autonomous weapons integrate several technologies into a unified system: sensors, data-processing units, pattern-recognition modules, decision-making algorithms, and executive subsystems for delivering force. Artificial intelligence allows these components to analyze the situation, adjust their reactions, and operate effectively in fast and highly dynamic environments.

Figure 3: Human-supervised autonomous weapons

Source: (Scharee, 2020)

Figure 4: Human-supervised autonomous weapons



Source: (Scharee, 2020)

According to the level of human involvement in decision-making, autonomous weapons fall into two categories (Scharee, 2020):

- Human-supervised autonomous weapons, where the operator remains "in the loop" and makes the final decision to attack (Figure 3).

- Fully autonomous weapons, where the entire engagement cycle—target search, detection, decision, and attack—unfolds without human intervention (Figure 4).

This distinction plays an important role in assessing the tactical value of autonomous weapons, as well as in identifying the risks they create. The level of autonomy determines the speed of decision-making, the possibility of human reaction, and the degree of control that armed forces can maintain over the system.

Understanding these characteristics forms the basis for correctly interpreting the capabilities and limitations of autonomous weapons in modern warfare. The combination of sensor technologies, data processing, and artificial intelligence algorithms reshapes the way weapons systems perceive the environment, make decisions, and execute tasks. For this reason, autonomous weapons have become a central topic in the analysis of modern military technologies and one of the most sensitive issues in evaluating their security, ethical, and tactical implications. Further analysis must examine the risks these systems generate and the conditions under which they can be used in a responsible and controlled manner.

3. Risks of Autonomous Weapons

Autonomous weapons introduce a new generation of military systems based on artificial intelligence and open a broad spectrum of technological, geopolitical, ethical, legal, and economic risks. These systems provide advanced capabilities but simultaneously create consequences that armed forces and international institutions struggle to predict and control. Their risks extend beyond traditional military considerations and include political, social, and economic implications. Autonomous systems operate through algorithms for pattern recognition, decision-making, and the execution of attacks, which makes their risks more complex than those of conventional weapons. Based on relevant literature and available research, this study identifies groups of risks that best illustrate the key challenges associated with autonomous weapons. These categories do not represent an exhaustive list, but they serve as the most significant groups for analysis within the scope of this paper.

Technological risks of autonomous weapons arise from their dependence on artificial intelligence algorithms, digital subsystems, and complex communication networks. A review of available literature highlights several key technological risks, although this list does not encompass all potential challenges. The most commonly identified risks include:

1. **Cyberattacks** – adversaries can manipulate algorithms, sensors, or communication channels, causing incorrect target identification, redirecting attacks, or disabling the system.
2. **Algorithmic errors and bias** – autonomous weapons depend on data quality and the reliability of AI models. Poor, incomplete, or misinterpreted data can lead to incorrect decisions.
3. **Technical failures and operational errors** – failures in sensors, guidance systems, or decision-making modules can trigger unintended reactions or result in a loss of functionality at critical moments.
4. **Loss of control** – the speed of autonomous decision-making can exceed the operator's ability to intervene, increasing the risk of unintended consequences and escalation.
5. **Dependence on complex AI architectures** – software vulnerabilities, attacks on algorithms, or coding errors can lead to unpredictable behavior or complete system failure.

Geopolitical risks of autonomous weapons arise from their potential to shift power balances, accelerate arms races, and increase uncertainty in international relations (Meiches, 2017). The use of AI-enabled autonomous systems affects political stability, security architectures, and the dynamics of conflicts between state and non-state actors. An analysis of relevant literature most commonly highlights the following geopolitical risks:

1. **Arms race** – the development of autonomous weapons motivates states to rapidly invest in new AI-driven military capabilities, which increases global tensions and reduces opportunities for diplomatic conflict resolution.
2. **Access by non-state actors** – increasingly accessible AI technologies raise the likelihood that autonomous systems will reach terrorist organizations or criminal groups, potentially destabilizing entire regions.
3. **Proliferation of technology** – the transfer of autonomous weapons to states with weak institutional capacities or to parties engaged in conflict elevates the risk of regional instability and violent escalation.

4. **Escalation of autonomous conflicts** – interactions between multiple autonomous systems on the battlefield can create rapid and uncontrolled conflict dynamics, as AI systems make decisions much faster than humans can respond.
5. **New competition in space and cyberspace** – autonomous systems used for surveillance, satellite reconnaissance, and cyber operations introduce new arenas of confrontation, with consequences that the global security framework struggles to anticipate.

Ethical and legal risks of autonomous weapons arise from the fact that algorithms take over decision-making processes that previously belonged exclusively to human actors. These risks include a range of dilemmas related to the protection of civilians, compliance with international humanitarian law, and the question of responsibility for decisions made by the system. An analysis of relevant literature most commonly highlights the following ethical and legal challenges:

1. **Collateral damage** – autonomous systems may misidentify targets due to algorithmic errors or insufficiently reliable data. This increases the risk of civilian casualties and the destruction of protected objects (Filipovic, 2023).
2. **Responsibility and accountability** – autonomous weapons raise the dilemma of who is accountable for the system's decisions: the commander, the programmer, the state, or the system itself. Current legal frameworks do not offer a clear answer to this issue.
3. **Limitations within international humanitarian law** – rapid technological development and high levels of automation exceed existing norms of international humanitarian law, creating legal gaps in regulating target selection and the use of force.
4. **Privacy intrusion and surveillance** – autonomous tracking and recognition systems may endanger individual privacy and raise ethical questions about the limits of surveillance in civilian and military environments.
5. **Information manipulation and disinformation** – autonomous systems, especially those relying on large datasets, can become tools for propaganda, psychological operations, or the dissemination of misleading content

Economic risks of autonomous weapons arise from the high costs of developing, producing, maintaining, and modernizing systems based on artificial intelligence. The use of these systems affects national budgets, international economic flows, and the long-term stability of states that invest in AI-driven military capabilities. Relevant literature most commonly highlights the following economic challenges:

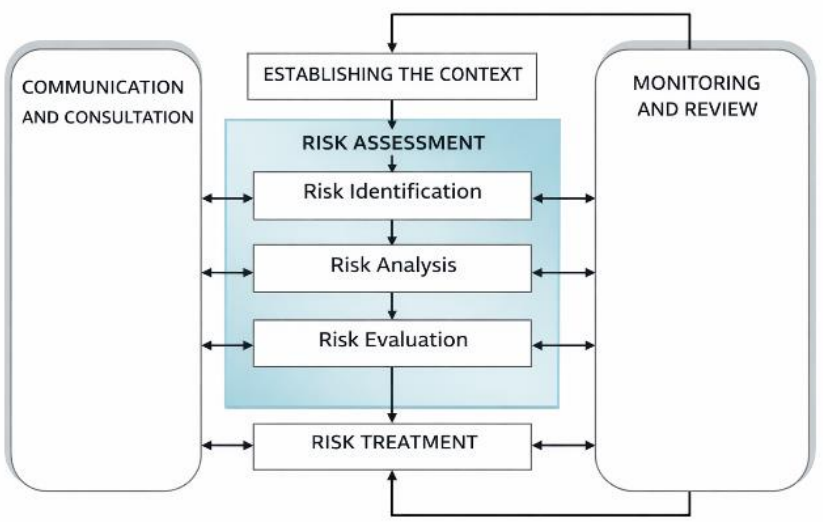
1. **High development and maintenance costs** – the creation and modernization of autonomous weapons require substantial financial investment in research, software modules, sensor equipment, and advanced communication systems, which can place significant pressure on military and state budgets.
2. **Impact on national and global economies** – large allocations for autonomous weapons may reduce funding for key public sectors such as healthcare, education, and infrastructure, affecting long-term economic development.
3. **Economic inequality among states** – wealthier states can invest in advanced AI-enabled military capabilities, while less developed states remain technologically inferior, deepening global security and economic disparities (Center for Strategic and International Studies, 2015).
4. **Market destabilization** – increased demand for AI-based military systems can fuel rapid and unregulated growth in the global arms market, creating opportunities for uncontrolled technology flows and illegal trade.
5. **Humanitarian and societal costs** – economic risks also include the long-term costs of post-conflict recovery, such as displacement of populations, health consequences, and the reconstruction of affected areas.

The analysis of technological, geopolitical, ethical, legal, and economic risks demonstrates that autonomous weapons fundamentally reshape the nature of modern warfare and the broader global security landscape. Although these systems offer significant operational advantages, their reliance on artificial intelligence creates layers of uncertainty that extend far beyond traditional military concerns. The risks identified in this chapter highlight the need for continuous assessment, transparent governance, and clearly defined international norms to prevent unintended escalation, misuse, or loss of control. Addressing these challenges requires coordinated action among states, international organizations, and the scientific community to ensure that the development and deployment of autonomous weapons remain aligned with principles of security, responsibility, and humanitarian protection.

4. Risk Management Model for Autonomous Weapons

The risk management process, defined by ISO standards, represents a systematic and interactive approach that aims to ensure effective and responsible management of risks associated with autonomous weapons (Jankovic & Komazec, 2024). These standards outline key steps that form the foundation of a proactive methodology in risk management. Figure 6 illustrates the risk management process and helps clarify how the different phases connect and contribute to the overall objective of managing risks.

Figure 6: Components of Autonomous Weapons



Source: (ISO 31000:2018)

The risk management process for autonomous weapons continually adapts to changes in technological development, political and social conditions, and the framework of international law. According to ISO 31000, the risk management process for autonomous weapons consists of five key phases:

Communication and Consultation: The process begins with open and continuous communication with all relevant stakeholders (Jankovic & Komazec, 2024; ISO 3100:2018). In the context of autonomous weapons, this phase involves engaging experts from military, political, technological, and other sectors, as well as representatives of governmental and international institutions, to ensure diverse perspectives and accurate information.

Establishing the Context: Clearly defining the external and internal parameters in which autonomous weapons are developed and used is essential for identifying potential risks. This includes considering political, legal, technological, and operational conditions that shape the environment of autonomous weapon deployment.

Risk Assessment: This phase includes Risk Identification, Risk Analysis, and Risk Evaluation. The assessment of risks related to autonomous weapons considers technological, geopolitical, ethical, legal, and economic risks, along with the probability of occurrence, the severity of consequences, and the overall level of risk.

Risk Treatment: In this phase, measures are implemented to manage, reduce, or eliminate identified risks. For autonomous weapons, this includes developing strategies that mitigate technological, geopolitical, ethical, legal, and economic risks. Each risk category requires specific treatment strategies (Table 1).

Monitoring and Review: Monitoring and review in the risk management process for autonomous weapons represent two essential components that ensure the overall effectiveness of the system (Jankovic & Komazec, 2024). Monitoring involves continuous observation and evaluation of the implemented risk management measures, including tracking technological developments, political conditions, and emerging threats. Review refers to the periodic re-examination of the entire risk management framework, which enables the identification of necessary improvements and alignment with new standards, regulations, and changes in the operational environment. This phase also includes assessing the effectiveness of autonomous weapons control measures and compliance with international agreements.

Table 1: Example Strategies for Managing Autonomous Weapon Risks

Risk Group	Example Strategies for Managing Autonomous Weapon Risks
Technological	- Enhance cybersecurity measures and conduct continuous threat monitoring. - Test algorithms, sensors, and decision-making modules before deployment. - Perform regular maintenance and AI model updates to reduce errors. - Implement double-check protocols before system activation. - Collaborate with technological institutions to improve AI robustness.
Geopolitical	- Strengthen diplomatic mechanisms for autonomous weapons control. - Participate in international agreements and oversight regimes. - Support intelligence-sharing to prevent misuse of autonomous systems. - Invest in confidence-building and transparency measures among states.
Ethical and Legal	- Define clear accountability norms for autonomous decision-making. - Align autonomous weapon development with international humanitarian law. - Establish oversight mechanisms for real-world deployment. - Minimize collateral damage and ensure civilian protection. - Increase transparency in development and operational use.
Economic	- Conduct cost-benefit analyses for AI military system adoption. - Plan budgets to avoid over-dependence on expensive AI systems. - Invest in post-conflict recovery programs. - Develop alternative economic sectors to reduce reliance on the defense industry.

Source: (author's elaboration based on the analysis of relevant literature)

The ISO 31000 risk management model for autonomous weapons supports their safe and responsible use. Each phase — from Communication and Consultation to Monitoring and Review — helps identify, analyze, and mitigate the risks associated with the development and deployment of autonomous weapons. Implementing targeted strategies for managing technological, geopolitical, ethical, legal, and economic risks provides the foundation for a sustainable and responsible approach in this field.

5. Conclusion

The analysis presented in this paper demonstrates that the integration of autonomous weapons into contemporary warfare introduces serious challenges that cannot be viewed solely through a technological lens. Autonomous systems, driven by artificial intelligence algorithms, generate risks far more complex than those associated with conventional weapons, as they introduce the possibility of loss of control, legally undefined responsibility, and the potential for unintended conflict escalation. At the same time, the geopolitical context and the ambiguity of international regulations further complicate predictable management of these systems. These risks require systematic understanding and governance, which this study enables through the identification of the most significant categories: technological, geopolitical, ethical, legal, and economic. Establishing such a spectrum of risks allows for a comprehensive assessment of the impact of autonomous weapons on security, civilian protection, and the stability of international relations. Additionally, this classification provides a foundation for practical strategies of control and risk mitigation. The ISO 31000 model, applied to autonomous weapons, offers a systematic framework that integrates all phases of risk management—from communication to monitoring and review. Continuous observation, system auditing, and revising measures in accordance with new insights ensure that risk management remains precise, effective, and aligned with relevant standards.

In conclusion, autonomous weapons cannot be treated merely as technological assets. The implementation of coherent and comprehensive risk-management strategies is a prerequisite for their responsible and safe use. Only through the integration of technical, legal, and ethical control mechanisms can the development and deployment of autonomous weapons be aligned with the principles of international law, humanitarian norms, and global security.

Literature

1. Center for Strategic and International Studies. (2025). Lessons from the Ukraine conflict: Modern warfare in the age of autonomy, information, and resilience. CSIS. Pristupljeno 25.12.2025. u 17:36 https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience
2. Filipovic, A. (2023). *Lethal Autonomous Weapon Systems (LAWS) – Towards Global Regulation or Indiscriminate Employment?* Political Review, No. 01/2023, Vol. XXXI(XXIII), p. 75.
3. International Committee of the Red Cross (ICRC). (2014). *Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects*. Expert Meeting, Geneva, Switzerland, 26–28 March 2014.
4. Janković, K., Komazec, N. & Mladenovic, M. (2025). *Dual Implications of Modern Armament in Contemporary Conflicts Through the Lens of Swot Analysis and The Ahp Method*. In Proceedings of the 11th International Scientific-Professional Conference "Security and Crisis Management – Theory and Practice (SeCMan)" (p. 253). RASEC & S4 Glosec Global Security. ISBN 978-86-80692-12-8
5. Janković, K., & Komazec, N. (2024). *Implications of modern weapons development*. In Proceedings of the 10th International Scientific-Professional Conference "Security and Crisis Management – Theory and Practice (SeCMan*)"* (p. 320). RASEC & S4 Glosec Global Security. ISBN 978-86-80692-11-1
6. Janković, K., & Komazec, N. (2024). *Upravljanje rizicima savremenog oružja*. In Zbornik radova sa Međunarodnog naučnog skupa „Savremeni izazovi i prijetnje bezbjednosti "(p. 161). Univerzitet u Banjoj Luci, Fakultet bezbjednosnih nauka. ISBN 978-99976-805-4-9.
7. Janković, K., Komazec, N., & Erkic, D. (2023). *Review of the risks of autonomous weapons*. In Proceedings of the 9th International Scientific-Professional Conference – Security and Crisis Management: Theory and Practice (SeCMan) (p. 54). Regional Association for Security and Crisis Management – RASEC, S4 GLOSEC Global Security. ISBN 978-86-80692-10-4.
8. Jončić, V. (2015). *International Humanitarian Law*. Faculty of Law, Belgrade.
9. Meiches, B. (2017). *Weapons, desire, and the making of war.* Critical Studies on Security, 5, 27-29. doi:10.1080/21624887.2017.1312149
10. Scharee, P. (2020). Vojska bez vojnika (Original work published as Army of None: Autonomous Weapons and the Future of War). Beograd: Laguna.
11. International Organization for Standardization. (2018). ISO 31000:2018 Risk management — Guidelines. ISO.