Publisher: Scientific-Professional Society for Disaster Risk Management

International Journal of Disaster Risk Management

Journal homepage: https://internationaljournalofdisasterriskmanagement.com

*Review Article*

# Implications of Artificial Intelligence and Cyberspace on Risk Management Capabilities

**Hatidža Beriša**[1,2], **Vanja Cvetković** [2*], **Aleksandar Pavić**[1]

[1] Military Academy, University of Defence, Veljka Lukića Kurjaka, 11042 Belgrade, Serbia, berisa.hatidza@gmail.com (H.B.).

[2] Scientific-Professional Society for Disaster Risk Management, Dimitrija Tucovića 121, 11040 Belgrade, Serbia, vanja.cvetkovic.drm@gmail.com.

*Correspondence: vanja.cvetkovic.drm@gmail.com

Received: 30 Juny 2024; Revised: 25 August 2024; Accepted 13 October; Published: 25 December

## Abstract

The crisis management system is a key element of a modern, reliable, effective, and sustainable security system. In contemporary settings, management functions are implemented through the capabilities of a command-information system. Consequently, most activities are conducted within cyberspace, meaning that management functions cannot be effectively executed without adequate telecommunications and information technology support. The primary target of hostile cyber activities is precisely the command-information system. Developing an optimal methodology for the use of command-information systems, as well as for prevention and protection against cyber-attacks, is among the most critical tasks for modern defence and security systems. One approach to enhancing risk management is through the application of artificial intelligence (AI). AI should ensure superiority in cyberspace, primarily at the national level, providing the foundation for executing legitimate and lawful cyber activities in a state's defence system. This paper aims to explore the role and significance of artificial intelligence within the realm of cybersecurity by analyzing its implications for risk management in contemporary environments. Command in modern military operations, the nature of modern warfare risks, the protection of command-information systems, the autonomy of artificial intelligence in decision-making, and an understanding of cyber threats are factors through which the challenges of modern command systems can be understood.

## Keywords

Artificial intelligence, autonomy, superiority in cyberspace, hybrid threats, risks, management

## 1. Introduction

The challenges of the modern command system within the defence framework have significantly evolved in the 21st century. Governance integrity in systems such as the military has always been a fundamental characteristic and structural pattern. The decision-maker stands as the central figure within a hierarchically organized system. Trust and accountability toward the system and its environment are vested in the commander or leader, who, through knowledge and authority, must

make decisions of utmost importance to the organization. The multidimensional nature of the contemporary operational environment presents leaders with numerous challenges. The risks faced by the modern defence and security system demand thorough consideration and analysis of all environmental (hazard) factors (Cvetković & Šišović, 2024; Cvetković, Renner, Aleksova, & Lukić, 2024; Cvetković, Čvorović, & Beriša, 2023a; Grozdanić & Cvetković, 2024), aiming to achieve timely and optimal decision-making. The core hypothesis of this paper is that the functioning of a management system in contemporary risks is unattainable without an understanding of cyberspace and artificial intelligence, as well as the utilization of their capabilities. This inherently drives us toward the integration and development of new competencies, supported by artificial intelligence capabilities, within systems that operate on a highly autonomous basis in a secure cyber environment.

The era in which activities increasingly shift from the visible domain to the information sphere and cyberspace presents a major challenge for leaders. Understanding the environment now requires a high level of abstraction and insight into hostile activities. On the other hand, technologies like artificial intelligence tend to assume part of the decision-making integrity traditionally held by leaders. The digital agenda—transferring a large number of activities into cyberspace and utilizing artificial intelligence—has created significant challenges for command systems. Although the use of artificial intelligence is widely accepted across various sectors of society, it is viewed with particular scrutiny in defence and security systems. Delegating a degree of autonomy to artificial intelligence in selecting targets and authorizing the use of lethal combat systems against humans confronts numerous ethical and legal concerns.

The primary aim of this paper is to explore the role and significance of artificial intelligence within the realm of risk management by analyzing its implications on risk management in contemporary crises. Despite the advanced technological capabilities and high interconnectivity brought by developments in the information and telecommunications sector, decision-making systems must be aligned and optimally positioned within this complex framework. To comprehend the challenges, risks, and threats faced by decision-making systems in today's environment, it is essential first to analyze and highlight the determinants of modern management systems, as well as the critical infrastructure within these systems. The challenges posed by the application of artificial intelligence in crisis and cyberspace represent a fundamental axiom influencing the capacity to execute management functions at the required level. A crucial segment to which the management system must respond in real time is AI-supported cyber activities. Mutual interaction in the 21st-century crisis field will demand the deployment of the most advanced technological capacities. Integrating human capabilities with artificial intelligence will be essential for achieving superiority in cyberspace and subsequently in other domains. Ultimately, how cyber threats and the use of artificial intelligence will impact management systems remains largely unknown, a question that the authors aim to partially elucidate in the following chapters.

## 2. Determinants of the modern management system

The concepts of crises have changed significantly. Regardless of the environment, technological development level, or crisis generation, two components remain constant: the involvement of humans as primary actors and management as the function that unifies all segments of risk (Cvetković & Šišović, 2023; Cvetković, 2024; Nikolić, Cvetković, & Ivanov, 2023). The shift in the crisis concept is primarily based on the ability to utilize the anthropological characteristics and features of nations and societies in determining the sources of conflict and transforming them into the fundamental causes and tools of what is now known as "modern crises." To understand some of the challenges faced by modern management, it is necessary to analyze the nature of contemporary crises, examine the protection of command-information systems, consider the level of artificial intelligence autonomy in decision-making, and comprehend cyber threats.

The challenges of modern risk management systems highlight the importance of integrating diverse approaches to address vulnerabilities across various domains. Akter, Roy, and Aktar (2023) emphasize the critical role of women in post-disaster health management, showcasing how gen-

der-specific challenges can hinder effective recovery processes. On the other hand, Goyal (2019) and Aleksandrina et al. (2019) explore systemic solutions, such as governmental incentivization and community resilience, as pivotal strategies to enhance disaster preparedness. In parallel, technological advancements in infrastructure monitoring and fire risk perception, as examined by Kachanov (2021) and Cvetković (2019), underline the need for robust systems that mitigate physical and cyber threats alike. Collectively, these studies contribute to a comprehensive understanding of disaster risk management by bridging social, systemic, and technological perspectives (Akter, Roy, & Aktar, 2023; Aleksandrina et al., 2019; Goyal, 2019; Kachanov, 2021; Cvetković, 2019).

Modern risk management systems in crises depend on various determinants that shape their structure and functioning (Cvetković, Sudar, & Ivanov, 2024; Cvetković, Andrić, & Ivanov, 2023). Key aspects include technology, education, communication, strategy, doctrine, leadership, and international cooperation (Jovičić, Gostimirović & Milašinović, 2024). These factors often interact with one another, forming complex risk management systems in contemporary crises. However, what primarily shapes the correlation of these factors are the challenges, risks, and threats faced by decision-makers, all of which have evolved alongside the risks over time.

### *2.1. Command-Information System*

The central role in all military systems is the implementation of the management function. The core element of a modern management system is the command-information system. This system comprises a set of hardware and software solutions that enable real-time integration of all organizational structures, doctrines, technical-technological systems and resources, information flows, and processes. Its purpose is to achieve efficient and rational functioning of the military as a whole, as well as its individual segments (Manjak & Miletić, 2011, pp. 78-93). It is an information system that supports management in crises at all levels, where data and information are collected, transmitted, distributed, processed, displayed, and protected. Disruption of the integrity and functioning of this information system directly impacts the operational capabilities of forces managing risks.

### *2.2. Cyberspace*

Various authors and organizations have attempted to define the concept of cyberspace. The primary fact is that cyberspace is simultaneously a source of cyber threats. However, it is undisputed that the essence of each definition is based on the same fundamentals. Cyberspace is understood as the "online" realm of computer networks, but also the digital world in general (Nedeljković, 2015). Cyberspace is created through technological and cybernetic means and represents a set of social relations that emerge when people begin to use computers, and when computers themselves start functioning as "assistive tools" for human activities. Cyberspace is an immaterial, artificially created world that is accessible to most. Not all rules are defined within it, which is why it is often described as both nobody's and everybody's property. It should not be confused with the internet, although they largely overlap. Cyberspace can exist within a single computer or other technical device, whereas the internet entails networking and communication (Vuletić, 2017).

Cyber threats are the result of malicious actors operating within cyberspace. Their actions harm information and communication systems that are the targets of cyber attacks. The sources of these threats can include states, corporations, specialized companies producing malicious software, dissatisfied individuals within the protected environment, terrorists, and botnet operators, and individuals who exploit the internet and social networks (Nedeljković, 2015). A similar principle can be applied to civilian command-information systems, which, like other systems of this type, are not immune to cyber threats.

### *2.3.The autonomy of artificial intelligence in the decision-making process*

The rapid development of artificial intelligence-based systems in recent years has led to a paradigm shift across various sectors, including defence. Modern weapon systems, with increased autonomy, can independently track, select targets, and act upon them without further human intervention. The application of artificial intelligence in this manner has the potential to revolutionize warfare due to capabilities such as autonomous decision-making, enhanced precision, and faster response times (Kenneth, 2018). These advantages can certainly lead to strategic superiority and a reduction in casualties. However, such weapons also raise significant international security and ethical concerns, underscoring the need for comprehensive global regulation within international institutions, particularly the United Nations.

The capabilities of artificial intelligence will undoubtedly have a deterministic and potentially transformative impact on military power, strategic competition, and global politics more broadly. It could be a generator of future uncertainty and vulnerability due to its rapid proliferation, as well as a potential source of instability and strategic rivalry among major powers (Johnson, 2019). Crises are generally conducted at all levels, with vast consequences that can produce strategic effects. Artificial intelligence will certainly play a role in some of these crises, through modern tools and as part of systems for operational planning and decision-making.

Today, we can increasingly envision a concept where artificial intelligence takes control over crisis management (https://www.military.africa/2023/11/artificial-intelligence-in-the-military). However, such concepts are the subject of discussion in various academic circles, which seek to find the boundary between reality and imagination. Although there are both negative and positive effects of artificial intelligence in military operations, the fact remains that its vectors of application are rapidly expanding. By analyzing various sources, the scope of AI use can be categorized into the following areas: autonomous armed combat platforms, strategic decision-making, data processing and analysis, combat simulation, target recognition, threat tracking, drone swarms, cybersecurity, transportation, casualty care, and evacuation (https://sdi.ai/blog/the-most-useful-military-applications-of-). Among the listed areas of application, cybersecurity stands out as particularly important for risk management systems in crises. With its analytical capabilities, scenario creation, and adaptability, artificial intelligence can enhance cybersecurity during crises. The command-information system, which is the core of management within civilian structures, is especially vulnerable in the domain of cybersecurity, as it represents critical infrastructure in modern crises.

Complete determination of management in modern crises, regardless of the technologies or solutions used—whether advanced artificial intelligence or automation systems—still depends on the human factor. Modern risk management systems, in their manifestation, can be characterized as complex adaptive systems.

Academic theorists and practitioners have an incomplete understanding of the complexity of complex adaptive systems, which will characterize the future operational environment for implementing management functions. Existing methods and ways of perceiving the operational environment will need to adapt to new trends. It can be concluded that the primary challenge, to begin with, is understanding how best to manage this process over time, considering the scope and nature of the transformation of risk management functions (https://assets.publishing.service.gov.uk/media/65c4dde79c5b7f0012951b35/Command_Control_Future_C2_Complexity.pdf).

## 3. Critical management infrastructure

The command and risk management system is one of the pillars that directly impact the reliability and effectiveness of defence and protection systems. This system must be fully functional in both peacetime and during emergencies. A critical point is always the transition from one state to another, especially when moving from a peacetime to an emergency organization. Although traditional emergencies are not as prevalent today, this does not imply that activities are not being conducted.

The formation of mobile and temporary components of the command-information system invariably represents a critical point vulnerable to cyber attacks. Modern risk management activities have accelerated with the use of artificial intelligence, leading to the application of deception measures and the dissemination of content within cyberspace. In the absence of adequate responses and measures to counteract malicious activities in cyberspace, such content floods digital media. Public trust in government institutions continues its long-term decline, and a growing sense of cynicism spreads, which significantly impacts defence capabilities (https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war). This can be explained by several factors.

First, the focus of operations shifts toward supporting military forces and conducting activities. Leadership structures concentrate on operational planning, developing new operations and branches of operations, and almost always overlook threats from cyberspace. It is often assumed that the command-information system will operate safely and reliably, which can lead to overlooking critical security aspects that impact the continuity and protection of communications. From this perspective, a disruption to system consistency can be more damaging than a temporary interruption. Second, during operations, part of the telecommunications equipment may be damaged due to disasters or theft. The loss of a platform with telecommunications equipment containing current cryptographic algorithms could open the door for access to a closed information system. This breach can then be exploited for cyber attacks, among other threats. Third, units connected via wireless communications are highly vulnerable to electronic interference. Such interference can completely or partially disable data transmission, significantly impacting the execution of assigned tasks. Fourth, there is a tendency among leadership to introduce the latest technological equipment, especially those with autonomous capabilities and no human crew. The introduction of such systems is very intensive today. Emphasis is always placed on their operational efficiency, while command-information systems are generally expected to ensure reliable communication for uninterrupted data transmission in the early stages of development. These systems, which are still in development, are often deployed to achieve an element of surprise or deterrence. However, this can also become a potential entry point into the command-information system.

The vulnerability of the command-information system is constant. Risk will always seek to find a weak point and attempt to disable parts or the entire system, as it is clear that without it, a management system in defence and protection does not exist. For this reason, it is essential to leverage the autonomous capabilities of artificial intelligence-based systems to prevent cyber attacks and potentially respond to cyber attacks. Unlike humans, artificial intelligence will not view the cyber segment as a peripheral system, especially during operations. Detecting attacks, identifying threats, and responding promptly are the foundations for defending the command information system.

## 4. Challenges of cyberspace and artificial intelligence

The national security of a state is now exposed to various challenges, risks, and threats, both conventional and unconventional. The shift from Cold War-era conventional and nuclear threats to an environment filled with elements of hybrid warfare—carried out in almost all phases within the cyber environment—poses a challenge for all nations. There is no defence system entirely immune to cyber threats (https://www.gao.gov/blog/u.s.-less-prepared-fight-cybercrime-it-could-be). The reason is simple: there is no single, dominant state system dictating activities in cyberspace; rather, it is now accessible to everyone. Cyber threats can be initiated by both state and non-state actors, extending to smaller groups and even individuals. An invisible attack from cyberspace is, above all, difficult to detect, and then challenging to counteract. When we add the capabilities of artificial intelligence to this, we get a very broad spectrum of possibilities. Whether artificial intelligence will develop to the point where it becomes the first non-human actor to independently execute a cyber attack remains uncertain, but to prevent this, robust protective instruments must be developed and utilized in the most effective way possible.

Artificial intelligence can be utilized to enhance cybersecurity during military operations in various ways. It can effectively detect threats and execute a preventive response to protect the system.

Detecting cyber attacks in real time is nearly impossible in modern information systems without high-tech support. Additionally, artificial intelligence can be used to identify vulnerabilities in military systems, which is crucial for preventing attacks before they occur. This may include developing new defense procedures and mechanisms. The final aspect focuses on improving training and planning within cybersecurity systems (Kaur, Gabrijelčić & Klobučar, 2023).

Military power is one of the fundamental components of each state's instrument of power. For this reason, the military is invariably an active target for those conducting cyber attacks. Today's armed forces are heavily developing numerous weapon platforms based on elements of artificial intelligence, aiming for greater autonomy in specific phases of engagement. The command-information system of the armed forces is the primary component that enables effective leadership and command at all levels. This system involves data transmission both horizontally and vertically, from the lowest to the highest levels. Additionally, information is transmitted across various media, through cables and increasingly through wireless channels. Commanding modern combat platforms, particularly at the tactical level, is impossible without advanced wireless communications. Despite typically being a leader in the realm of protection and attack prevention methods, the military command-information system remains an attractive target for various cyber attacks.

Cyberspace and artificial intelligence are two inseparable segments of the modern operational environment. The first important factor relates to the breadth and comprehensiveness of cyberspace. It spans from individuals using smart devices in nearly all activities to the highest national level that integrates all aspects of a state's functioning. Modern electronic communications occur entirely within cyberspace. The challenges, risks, and threats arising from cyberspace are real and daily. The second crucial factor that aims to influence our environment comprehensively is artificial intelligence. Its development and rapid global spread would not be possible without cyberspace. Artificial intelligence, without access to cyberspace, can only perform basic tasks defined by a limited dataset and an installed algorithm. To learn, it must be continually updated with new data and interact with other entities. Artificial intelligence that operates freely in cyberspace has the essential precondition for growth and learning. For this reason, artificial intelligence can be seen as a system that acts preventively against malicious activities in cyberspace but can also serve as a generator of threats.

The future of crisis management will undoubtedly be shaped by systems that utilize artificial intelligence and cyberspace. Modern disasters are practically unimaginable without the dimension of cyberspace and technologies based on artificial intelligence ( https://www.rand.org/pubs/commentary/2022/11/ukraines-lessons-for-the-future-of-hybrid-warfare.html). A broad range of risks is manifested through various activities, including cyber activities, conventional military actions, economic, and social interventions (Sanz-Caballero, 2023). The weapons used in these activities could include computers, drones, mass media, hijacked airplanes, spy balloons, as well as artificial intelligence. An incomplete list of hybrid threats would also include cyber attacks, terrorism, organized crime, drug trafficking, migration flows, economic or financial warfare, media exploitation, and the use of covert psychological operations (Galan, 2018).

A crucial segment related to cyberspace is gaining importance, particularly because all states are digitizing their administration and operational agendas. This segment also includes military organizations. It can be said that modern state apparatuses could not function without cyberspace and information technologies. Although cyber threats are diverse, they represent a significant source of risk for the modern state, and therefore for the defense system as well. Modern threats are mostly invisible, and by the time their effects become apparent, it is often too late for an effective defense.

The use of artificial intelligence is increasingly shifting modern crises from conventional to cyber space. Although we cannot entirely abandon the principles of the conventional domain, as this type of threat remains the dominant form of operations, artificial intelligence is becoming an integral part of various platforms—from lethal autonomous platforms and systems that perform analytical tasks and data processing, to decision-making and operational planning processes. The wide range of AI applications, from tactical to strategic levels, ensures its development and presence in all aspects of operations.

The shift from automation toward autonomy will require exceptionally high system reliability (Scharre, 2006). One potential response to this challenge is the development of high-reliability organizations, which demonstrate certain characteristics enabling them to routinely manage high-risk systems with low accident rates. High-reliability organizations can be found across various fields and share common characteristics. These include not only highly trained individuals but also a collective awareness of risks and a continuous commitment to learning (Sutcliffe & Sutcliffe, 2015). The reliability of autonomous systems should be one of the core principles for organizations that utilize them.

The command-information system in all defense systems is the backbone for executing assigned missions and tasks. The part of the system responsible for transmitting digitized data and commands is stationed in cyberspace and, as such, is inevitably a target for cyber attacks. A pertinent question arises regarding the role of artificial intelligence in cyberspace—will artificial intelligence serve as part of the defense system, or will it be used to conduct cyber attacks (https://www.piranirisk.com/blog/artificial-intelligence-to-combat-cyber-attacks#:~:text=The%20use%20of%20artificial%20intelligence,materialization%20of%20cyber%20attacks%2C%20which). This is one of the significant challenges that cybersecurity components of defense systems will face. Artificial intelligence has the potential to make military systems more secure, resilient, and efficient, but it also introduces new challenges and risks (Jan Maarten, 2023).

## 5. Artificial intelligence in cyber operations

A significant advancement in the use of artificial intelligence will be its potential application in cyber operations. Whether offensive or defensive, these applications will undoubtedly have substantial effects. The capability to design and execute cyber-attacks faster and more efficiently than humans presents a major challenge for future cybersecurity. These operations are not limited to digital domains but extend to physical assets, including weapons and support systems. Potential targets of cyber operations include all systems and installations connected to cyberspace (https://www.aspistrategist.org.au/the-impact-of-artificial-intelligence-on-cyber-offence-and-defence/).

The definitions of cyber operations have evolved in line with technological advancements and changes in doctrine. Among others, Department of Defense Publication 3-12 of the United States outlines these definitions as "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace" (https://irp.fas.org/doddir/dod/jp3_12.pdf). A cyber operation consists of computer network attacks, computer network defense, and related operations that enable the exploitation of computer networks. This implies that the core tasks of cyber defense are: identifying threats, mitigating the impact of threats, and carrying out activities to counteract the consequences of threats (Doktrina kopnene vojske, 2012).

Examples include hacker attacks supported by Iran in 2012, as well as the Russian military intelligence attack in December 2015, which conducted a destructive cyber attack on Ukraine's power grid, leaving much of the country in darkness. Another example of an attack on a closed information system is the notorious "STUXNET" virus, which disabled centrifuges at a nuclear facility. All these examples are part of cyber operations that, through cyberspace, impacted the vital systems of the targeted state (https://www.iemed.org/publication/artificial-intelligence-machine-learning-and-cyber-command-as-a-tool-of-war-a-new-method-in-the-mediterranean-battlefield/). What these examples have in common is that the infrastructure of the information system was attacked, directly affecting the ability to command within the system. This is significant in the military context, as the inability to relay orders and commands to executing elements on the battlefield directly impacts the outcome of an operation. On a broader scale, it can completely paralyze the military's command-information system.

The previously mentioned examples demonstrate that the implications of cyber warfare can have global effects. Warfare is no longer confined to physical battlefields with soldiers; it has become an integral part of the digital domain, or cyberspace. The digital extension of global conflicts and proxy wars illustrates how cyber warfare has become an essential component of international relations and security.

In a RAND Corporation report titled "Cyber War is Coming!" as early as 1993, the author discussed the prospects of future warfare. Cyber warfare is described as an "information revolution" in which outcomes are no longer determined by kinetic elements or mobility but by strategic cyber operations. This environment enables powerful actors to compete indirectly, emphasizing a shift from traditional confrontation to more covert operations (https://www.rand.org/pubs/reprints/RP223.html). Such an approach aligns with the theory of strategic interaction, which emphasizes the shifting nature of global conflict (Arreguín-Toft, 2001).

Cyber warfare represents a significant shift in the way global conflicts are conducted. The rise of artificial intelligence in cyber operations, the information revolution, the digital evolution of warfare, the need for international norms, and the comprehensive impact of technology on society together create a vision of a future where cyber warfare is an integral part of international relations and security (https://medium.com/@mikevfuentes/the-future-of-cyber-warfare-1ad1a9a66d0c).

Future cyber operations will undoubtedly be enhanced by the capabilities of artificial intelligence. Whether defensive or offensive, such operations will become increasingly prevalent on the battlefield. The readiness of defense systems to implement new technologies to improve the command-information system is essential for effective attack prevention and for preserving the integrity of command functions. Dominance in cyberspace will become a key indicator of operational outcomes and a state's ability to defend itself not only in cyberspace but across other dimensions as well. In the following chapters, the authors will attempt to examine the challenges of AI operations in cyberspace, future concepts of conducting military operations, and ultimately, to model elements of cyber activities.

## 6. Integrating artificial intelligence into the management process

The integration of AI-supported technologies into the protection system can be achieved through the development of necessary capabilities and doctrinal structuring of usage methods. Key capabilities for management can be examined from three perspectives within the context of this study. The first pertains to the degree of autonomy of artificial intelligence in the decision-making process. The second aspect involves the prevention of cyber attacks on the command-information system, which is the primary support for risk management functioning in a crisis. Finally, the third aspect of integrating artificial intelligence should ensure the supremacy of AI in the risk management process during activities.

### *6.1. Autonomy and Cybersecurity*

The military, as a driver of new technology development and implementation, has already widely adopted the use of artificial intelligence. The broad range of AI applications, as well as theoretical considerations of its potential uses, ultimately brings us to the question: How much autonomy can we allow artificial intelligence in military applications? This question extends beyond the military but is particularly compelling within defence systems, as only there could AI potentially gain autonomy in deploying lethal combat systems against humans. This ethical and legal dilemma is increasingly relevant as the use of AI in military contexts expands. However, artificial intelligence has a much broader scope beyond executing individual combat systems; it presents a significant opportunity for optimizing decision-support processes in decision-making and operational planning ( Meerveld et al, 2023). This possibility leads us to the question of responsible use of artificial intelligence in the military, specifically concerning the delegation of a portion of responsibility and decision-making authority.

The defence and protection system, particularly its most critical operational component—the civil protection system—conducts its actions and activities according to doctrine. New challenges in risk management, especially within the domain of cybersecurity, necessitate the development of new capabilities. Artificial intelligence, with its broad range of possibilities, will undoubtedly serve

as a significant tool in developing the capabilities of forces, not only in the cyber domain but also in other aspects of force application. Part of these capabilities should include the ability to detect cyber attacks promptly, notify responsible personnel, and implement countermeasures. Cybersecurity faces increasingly complex challenges due to advances in information technology and artificial intelligence. The key question in capability development is whether it is justified to have artificial intelligence alongside humans in the decision-making loop or if, in the future, it will completely replace humans in the loop.

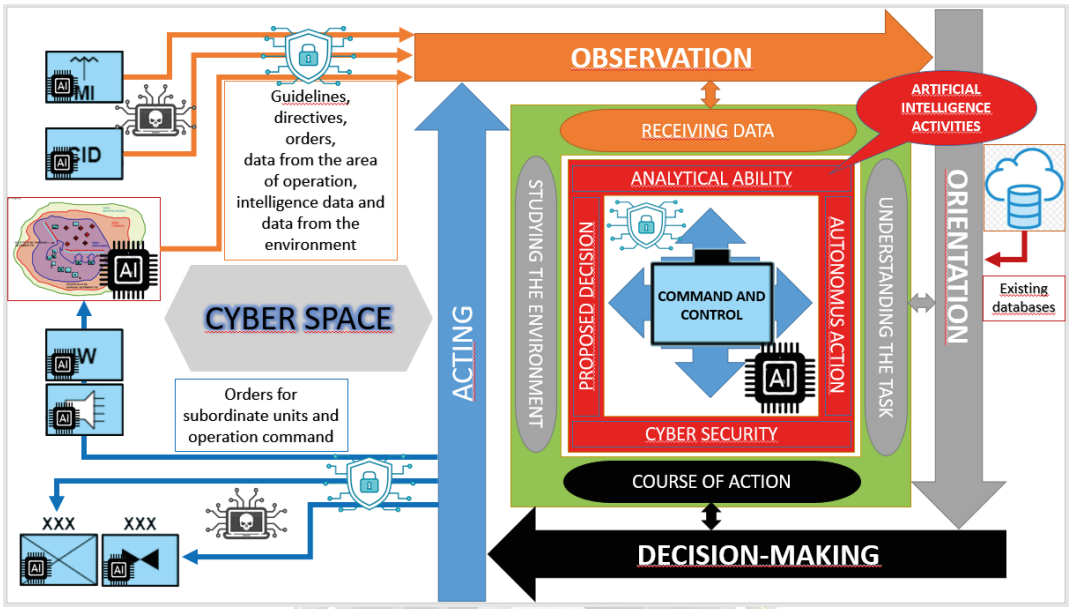


Figure 1 illustrates the modern complex operational environment in cyberspace. Artificial intelligence primarily executes tasks within the decision-making process, providing decision support. Positioned within the OODA decision loop alongside humans, AI enhances the speed of decision-making with its capabilities. In addition to its placement in the command center, artificial intelligence can also be integrated into tactical-level combat platforms, which require control and direction for new tasks. These assigned tasks include receiving data from sensors and managing autonomous combat systems on the battlefield by relaying engagement orders. Another segment of activity involves cybersecurity—specifically detection, notification, and counter-response to cyber attacks. The command-information system in cyberspace encompasses all combat power entities within a unified system, constantly exposed to cyber attacks during operations. The modern operational environment shown in Figure 1 suggests that clear coordination between the command system, cyberspace control, and AI-utilizing entities is essential. Such coordinated use ensures superiority in cyberspace and provides the fundamental prerequisite for the secure continuation of other combat activities.

The introduction of artificial intelligence into operational use within the defense and protection system requires doctrinal structuring that must align with the objective capabilities and new competencies of the forces. Without doctrine, it is impossible to effectively and optimally deploy forces that utilize AI resources in operations. For the doctrine to be fully applicable, it requires the necessary capabilities and specific knowledge about how to employ those capabilities ( Ostojić, Karavidić & Projović, 2017).

### *6.2. Supremacy of Artificial Intelligence*

The development of combat platforms integrating artificial intelligence capabilities has been evident for many years. The primary goal of integrating artificial intelligence should be to achieve supremacy over the adversary. Enhancing the performance of Boyd's OODA (Observe, Orient, Decide, Act) cycle in decision-making is one of the key factors in securing supremacy. Examining the role and position of artificial intelligence within the processes of observation, orientation, decision-mak-

ing, and action is essential for its integration into operations. Another critical factor in integration is a doctrinal framework that is aligned and prepared for use in modern operations. An inadequate doctrine for employing forces equipped with the latest technologies can negate all the advantages of modern autonomous systems.

The automation of processes in operations is not new; it has been systematically used for decades. Multi-sensor networks, the digital age rich with vast amounts of data stored across numerous databases, advanced algorithms for data processing, and decision support are all part of an agenda that requires high levels of process automation to provide real-time support to decision-makers.

Countries that maintain a technological edge, such as the United States, the People's Republic of China, the Russian Federation, and others, are leaders in the application of new and revolutionary technologies. The increasing use of autonomous combat systems is a clear example. From unmanned aerial vehicles to loitering munitions, automated combat vehicles, and tactical weaponry, all these systems significantly enhance the combat capabilities and operational effectiveness of units and the military as a whole. However, various indicators suggest that the adoption of these technologies will reach its full potential alongside advancements in the information agenda. The use of autonomous systems heavily relies on human potential for system maintenance and the processing of data generated by these systems (Mayer, 2023).

The development of the information age and the emphasis on the importance of cyberspace should serve as a new guideline for integrating artificial intelligence into future operations. Management across all systems requires a swift flow of information and the transmission of orders to subordinate units. In this process, artificial intelligence should act as a generator of progress. Another important factor is the security of cyberspace, which must ensure integrity, a high level of reliability, and the protection of information. The ability to fully integrate information gathering, communication, storage, and processing into timely and decisive action can result in new technological and conceptual advantages. These technologies, embodied in artificial intelligence and the development of autonomous systems, can cumulatively lead to what may be termed the "Third Offset" (Gian et al, 2021).

To fully leverage the advantages of artificial intelligence and autonomous systems, a more advanced integration into the decision-making process will be required. Additionally, significant influence on the previously stated position must be accompanied by trust in their ability to operate without human intervention. A key factor that arises here is who is authorized to make decisions. An interesting example can be illustrated with two highly automated systems used by the U.S. military (https://thebulletin.org/2021/04/worried-about-the-autonomous-weapons-of-the-future-look-at-whats-already-gone-wrong/). Specifically, the automation of the Patriot air defense system is designed to replace human involvement in the decision-making process and to independently respond to detected threats. Another significant system is Aegis, used by the Navy, which primarily aims to utilize automation to facilitate the commander's decision-making using appropriate doctrine. Of course, in both systems, there is the possibility for humans to control all options; however, there is also the potential for both to respond completely autonomously to identified threats. Another crucial factor influencing the decision-making process is the doctrine employed. A universal doctrine that consistently responds to the same threats in the same manner has many shortcomings that manifest in different circumstances. This implies that the complexity of using autonomous systems necessitates a corresponding doctrine that is aligned with the appropriate operational environment.

The speed that dominates Boyd's OODA loop is not always the primary factor that determines victory. Doctrine, environment, reliability, and adequate assessment should precede the correct decision regarding the use of combat power. Artificial intelligence integrated into Boyd's loop can be an ideal tool for exploring the performance of combat systems. The combination of human involvement and artificial intelligence in the loop is certainly a desirable and fully controlled system. The intuitive steps of the OODA loop are easily understood and closely aligned with the first four fundamental elements of artificial intelligence: perception, understanding, prediction, and manipulation, or learning (Johnson, 2023).

The integration of delegating autonomy to artificial intelligence and achieving supremacy in cyberspace are factors that will undoubtedly play a crucial role in the execution of military operations

in the future. They will directly reflect on the quality of command functions. The fight against a modern digital adversary operating in hybrid warfare is only possible by ensuring complete functionality and flexibility in command, which can only be achieved through the implementation of cutting-edge technological solutions.

## 7. Impact of cyber threats on crisis management

Using existing methods and knowledge, it is nearly impossible to ascertain the actual impact of cyber attacks on achieving objectives during a crisis (Musman, Scott & Temin; Aaron & Tanner; Mike & Fox; Dick & Pridemore, 2010). When considering the direct impact of cyber attacks on an ongoing crisis, it is essential to address several questions to undertake appropriate preventive actions before the crisis begins or to mitigate the consequences during its execution. Questions may include: Are we aware of which elements of the operational deployment are affected? Can we continue managing the ongoing crisis while under a cyber attack? Is it necessary to wait for the cyber attack to cease and for the damage to be rectified before resuming activities? Is it possible to mitigate damage during the crisis? Decision-makers often find it challenging to comprehend and assess the impact of a cyber incident on operations, which diminishes their ability to respond effectively. The very framework for the execution and impact of cyber attacks introduces significant uncertainty within organizations, resulting in responses that are generally misaligned and delayed. Enhancing awareness of the effects of cyber attacks on civil protection crises will undoubtedly lead to improved responses and the creation of systems that are more resilient to attacks.

Within the capacity for effective and efficient use of forces, cyber threats can be viewed as a set of activities that threaten to diminish the effectiveness of the forces and slow down the execution of assigned missions and tasks. Following this, it is essential to focus the work on assessing the impact of cyber attacks and to prepare a set of countermeasures aimed at protecting the forces and the infrastructure critical for conducting operations (Aljundi, Ibrahem & Rawashdeh; Morad & Al-Fayoumi; Mustafa & Al-Badarneh; Amer & Abu Al-Haija, 2023). To that end, it is essential to connect the capabilities of information technologies with the execution of strategies, specifically with measures that directly impact the effective and efficient use of forces. Understanding the critical requirements and capabilities necessary for executing assigned tasks is key, as well as knowing the activities that fulfil the needs of the assigned mission, the supporting cyberinfrastructure, and comprehending how the effects of attacks alter the course of a crisis.

The increased integration of computers and information technologies into crisis management processes has created an environment where compromising, damaging, or losing information and telecommunications infrastructure can lead to the failure of the entire crisis operation. Our expectations for the success of an operational group/unit under an active cyber attack—specifically an attack on the information and telecommunications infrastructure supporting the crisis—largely depend on understanding how a cyber attack degrades capabilities in the kinetic space. The kinetic space should be considered alongside all other infrastructure that is not related to the information and telecommunications segment.

In real actions, when a rapid response to an imminent threat is necessary, a commander may need to decide on the use of resources to neutralize that threat. The ability of commanders to select a means of responding to a disaster threat, for example, depends on the information about available resources both in the air and on the ground. Any type of resource can be useful depending on the target type. However, if at any point access to data about the systems or the management information system is lost, it will certainly impact the response. The sources of the problem can vary. If cyber attack detection systems identify certain activities on critical network equipment aimed at degrading functionality or ceasing operations, it can be concluded that a cyber attack has occurred on the information system or a part of it. One common example is the classic „DDoS" attack. Once it is established that the system is under attack, we still do not know what the ultimate target of the attack is or when it will end. All of this can significantly impact the final objective of force engagement and the achievement of the desired end state. The commander may decide to continue operations

with the resources available until the consequences of the cyber attack are resolved. From this, we can conclude that an indirect attack can be equally effective as a direct attack on the combat system itself. In both cases, the ability to counteract the source of the threat is temporarily disabled.

The previously mentioned practical example necessitates that modern crisis planning includes the need for protective measures and countermeasures against attacks on information infrastructure. Forces and resources in a crisis must be protected across all segments, as an asymmetric approach to conducting operations is pervasive, and all sources of direct threats must be thoroughly analyzed.

Currently, we have very few capabilities to assess the impact and effects of cyber incidents on the execution of operations. The analysis of the dependencies between objectives, missions, crisis tasks, and information-telecommunication resources is not common. During the operational planning process, the information network is rarely considered as an aspect from which a threat may arise. An exception occurs in crises that intentionally utilize cyberspace as a venue for risk, such as information crises. In all other cases, even if a risk is identified, it is generally deemed to be of minor importance to the outcome of the crisis and is not analyzed in detail (Grimaila & Fortson, 2007). If we consider a threat from cyberspace, it is possible to undertake certain preparations through the following steps (https://www.dnv.com/cybersecurity/cyber-insights/recognizing-the-seven-stages-of-a-cyber-attack/):

1. Assessing the dependencies between cyberinfrastructure and activities during the execution of tasks and the achievement of crisis objectives;
2. Determining the impact of cyber attacks on the crisis based on the timing and duration of the incident;
3. Analyzing and forecasting the impact of cyber threats on resources that are currently not in use;
4. Forecasting the impact of future operational branches and potential future crises.

The previously mentioned steps inherently set the requirements for the discovery and use of appropriate techniques to combat cyber threats. Here, it is essential to emphasize the importance of real-time response, as it is the only way to influence malicious cyber activity and prevent its impact on the execution of operations.

Since formal assessments of cyber risks occur during offline evaluations, they focus on the potential cyber effects against a wide range of possible threats. The effects of cyber attacks can be classified into the following categories: degradation of system characteristics, disruption of system operations, modification of system functions, user deception, unauthorized access to the system, and data interception (https://www.dnv.com/cybersecurity/cyber-insights/recognizing-the-seven-stages-of-a-cyber-attack/ ; Singh et al, 2011).

Damage analysis is an integral part of addressing the consequences of cyber attacks and, in addition to direct access, requires additional analysis and planning of preventive measures for future crises. It can be presented as a system of lessons learned. An important characteristic of assessing the impact of a given threat is its temporal nature. Time is a more significant factor than understanding the current capabilities of the information system when a cyber attack begins. It is essential to be able to anticipate threats or at least to configure the system so that vital functionalities are not compromised after an attack. Effective impact assessment involves understanding the exhibited activity, whether it is planned or based on expectations. Anticipated activity indicates what is likely to be lost in the event of a failure of defense or degradation of the part of the system that is under attack. It is also worth considering that depending on where and how the components of the information system are based, there may be an opportunity to monitor activity, that is, the effects of the attack, from the monitoring center. When the team actively working against the attack or simply monitoring it is well trained and equipped, if they timely detect the absence of the attacker, it can create an opportunity for a counterattack. If there is no capability for an effective and efficient response to the threat, it will certainly lead to an assessment of jeopardizing the entire operation and take preventive action to activate backup resources.

The challenge of assessing the impact of cyber attacks lies in the process of connecting the mission of crisis operations with the information and telecommunications infrastructure to support and

understand those relationships. An operation is viewed as a set of activities that must be carried out to accomplish the assigned task. Activities are executed using allocated resources, including the information and telecommunications infrastructure. During these activities, various types of information are exchanged, created, or utilized. Resources from the domain of information technology are allocated to users according to their needs, typically involving specific equipment that enables information exchange during the execution of combat operations.

## 8. Conclusion

The risk management system in modern civil and military organizations will, despite all the challenges they face, maintain a central role and significance in leadership at all levels. The automation of activities at various levels, along with the autonomy of certain combat systems, will undoubtedly contribute to making future military operations more efficient and effective. Increased precision, speed, and optimization resulting from the use of artificial intelligence should lead to crises being resolved with fewer casualties and less destruction, aligning with the international legal agenda and the ethical standards of the modern world. The cyber domain, as one of the most important sources of power in the 21st century, must ensure a secure management environment that provides decision-makers with an advantage and facilitates the timely and safe transmission of orders and essential information.

The challenge of utilizing high technologies integrated through the cyber agenda and artificial intelligence in risk management systems presents various advantages as well as certain uncertainties. The positive effects are reflected in the acceleration of the decision-making process, optimization of activities through reduced resource expenditure, and ultimately a shorter duration of crises. On the other hand, the uncertainties regarding the development vectors of artificial intelligence, particularly in terms of autonomy and the assumption of responsibilities currently exclusive to humans, will significantly shape future command systems. The dispersal of power among various actors, including non-state ones, will lead to a changed distribution of power from the national level, through the regional, to the global level.

The modern concept of management will primarily influence the enhancement of national security systems. As a rule, most malicious activities will first emerge from cyberspace and then from other dimensions. The superiority of cyberspace provides an advantage to risk management systems about contemporary risk and threat challenges, and the development of intelligence should facilitate this. Future leaders need to study, implement, and utilize modern technologies, as only then can they provide timely responses to contemporary risk and threat challenges through command systems. The most significant challenge is to achieve synchronization and correlation between natural and artificial intelligence. This means that humans must always be the ones making the final decisions, while also delegating tasks and responsibilities to artificial intelligence that do not compromise the command integrity of humans.

**Acknowledgements:** The authors acknowledge the use of Grammarly Premium and ChatGPT 4.0 in the process of translating and improving the clarity and quality of the English language in this manuscript. The AI tools were used to assist in language enhancement but were not involved in the development of the scientific content. The authors take full responsibility for the originality, validity, and integrity of the manuscript.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References


1. Akter, R., Roy, T., & Aktar, R. (2023). The Challenges of Women in Post-disaster Health Management: A Study in Khulna District. International Journal of Disaster Risk Management, 5(1), 51-66.
2. Aleksandrina, M., Budiarti, D., Yu, Z., Pasha, F., & Shaw, R. (2019). Governmental Incentivization for SMEs' Engagement in Disaster Resilience in Southeast Asia. *International Journal of Disaster Risk Management, 1*(1), 32-50.
3. Aljundi, I., Rawashdeh, M., Al-Fayoumi, M., Al-Badarneh, A., & Abu Al-Haija, Q. (2023). Protecting critical national infrastructures: An overview of cyber attacks and countermeasures.
4. Al-ramlawi, A., El-Mougher, M., & Al-Agha, M. (2020). The Role of Al-Shifa Medical Complex Administration in Evacuation & Sheltering Planning. *International Journal of Disaster Risk Management, 2*(2), 19-36.
5. Arreguín-Toft, I. (2001). How the weak win wars: A theory of asymmetric conflict. *International Security, 26*(1), 93–128. http://www.jstor.org/stable/3092079.
6. Australian Strategic Policy Institute. (2024, March 22). *The impact of artificial intelligence on cyber offence and defence*. Retrieved March 22, 2024, from https://www.aspistrategist.org.au/the-impact-of-artificial-intelligence-on-cyber-offence-and-defence/.
7. Bulletin of the Atomic Scientists. (2021, April). *Worried about the autonomous weapons of the future? Look at what's already gone wrong*. Retrieved March 17, 2024, from https://thebulletin.org/2021/04/worried-about-the-autonomous-weapons-of-the-future-look-at-whats-already-gone-wrong/.
8. Center for Strategic and International Studies (CSIS). (n.d.). *Cyber operations during the Russo-Ukrainian war*. Retrieved March 22, 2024, from https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.
9. Command and Control: Future C2 Complexity. (n.d.). Retrieved March 22, 2024, from https://assets.publishing.service.gov.uk/media/65c4dde79c5b7f0012951b35/Command_Control_Future_C2_Complexity.pdf.
10. Cruz, R. D. D., & Ormilla, R. C. G. (2022). Disaster Risk Reduction Management Implementation in the Public Elementary Schools of the Department of Education, Philippines. International Journal of Disaster Risk Management, 4(2), 1-15.
11. Cvetković, V. & Šišović, V. (2023). Capacity building in Serbia for disaster and climate risk education. Disaster and Climate Risk Education Insights from Knowledge to Action, edited by: Ayse Yildiz and Rajib Shaw, book series Disaster Risk Reduction, Springer Nature Singapore Pte Ltd., 152 Beach Road.
12. Cvetković, V. (2019). Risk Perception of Building Fires in Belgrade. International Journal of Disaster Risk Management, 1(1), 81-91.
13. Cvetković, V. (2024). Empowering the Regional Network of Experts for Disaster Risk Management in the Western Balkans by the Scientific-Professional Society for Disaster Risk Management. International Scientific and Practical Conference: "International Experience in Emergency Risk Management" in Moscow, Russia.
14. Cvetković, V. M., Tanasić, J., Ocal, A., Kešetović, Ž., Nikolić, N., & Dragašević, A. (2021). Capacity Development of Local Self-Governments for Disaster Risk Management. *International Journal of Environmental Research and Public Health, 18*(19), 10406.
15. Cvetković, V. M., & Šišović, V. (2024). Understanding the Sustainable Development of Community (Social) Disaster Resilience in Serbia: Demographic and Socio-Economic Impacts. Sustainability, 16(7), 2620.
16. Cvetković, V. M., Renner, R., Aleksova, B., & Lukić, T. (2024). Geospatial and Temporal Patterns of Natural and Man-Made (Technological) Disasters (1900–2024): Insights from Different Socio-Economic and Demographic Perspectives. Applied Sciences, 14(18), 8129.
17. Cvetkovic, V. M., & Martinović, J. (2020). Innovative solutions for flood risk management. International Journal of Disaster Risk Management, 2(2), 71-100.

18. Cvetković, V., Andrić, K., Ivanov, A. (2023). Comparative Analysis of Disaster Risk Management Systems in Germany, USA, Russia And China. Macedonia. International academic conference, Temporary security ripples or new world architecture of security, Dojran, N. Macedonia, September 4-7 2023.
19. Cvetković, V., Čvorović, M., & Beriša, H. (2023a). The Gender Dimension of Vulnerability in Disaster Caused by the Corona Virus (Covid-19). NBP, 28(2), 32-54.
20. Cvetković, V., Sudar, S., Ivanov, A. (2024). Harmonization of Soft Power and Institutional Skills: Montenegro's Path to Accession to the European Union in the Environmental Sector. International Journal of Disaster Risk Management, 6(1), 41–74.
21. DNV. (2024, March 22). *Recognizing the seven stages of a cyber attack*. Retrieved March 22, 2024, from https://www.dnv.com/cybersecurity/cyber-insights/recognizing-the-seven-stages-of-a-cyber-attack/.
22. *Doktrina Kopnene vojske* [Doctrine of the Army]. (2012). Medija centar "Odbrana", Beograd.
23. El-Mougher, M. M. (2022). Level of coordination between the humanitarian and governmental organizations in Gaza Strip and its impact on the humanitarian interventions to the Internally Displaced People (IDPs) following May escalation 2021. International Journal of Disaster Risk Management, 4(2), 15-45.
24. Fuentes, M. V. (2024, March 22). *The future of cyber warfare*. *Medium*. Retrieved March 22, 2024, from https://medium.com/@mikevfuentes/the-future-of-cyber-warfare-1ad1a9a66d0c.
25. Galán, C. (2018). Amenazas híbridas. Nuevas herramientas para viejas aspiraciones. *Elcano Documentos de Trabajo, 20/2018*, 3.
26. Gentile, G., Shurkin, M., Evans, A. T., Grisé, M., Hvizda, M., & Jensen, R. (2021). *A history of the Third Offset, 2014–2018*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA454-1.html.
27. Goyal, N. (2019). Disaster governance and community resilience: The law and the role of SDMAs. International Journal of Disaster Risk Management, 1(2), 61-75.
28. Grimaila, M. R., & Fortson, L. W. (2007). Towards an information asset-based defensive cyber damage assessment process. In *Proceedings IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2007)*.
29. Grozdanić, G., Cvetković, V. (2024). Exploring Multifaceted Factors Influencing Community Resilience to Earthquake-Induced Geohazards: Insights from Montenegro. Belgrade: Scientific-professional Society For Disaster Risk Management.
30. IEMED. (2024, March 22). *Artificial intelligence, machine learning, and cyber command as a tool of war: A new method in the Mediterranean battlefield*. Retrieved March 22, 2024, from https://www.iemed.org/publication/artificial-intelligence-machine-learning-and-cyber-command-as-a-tool-of-war-a-new-method-in-the-mediterranean-battlefield/.
31. Johnson, J. (2019). Artificial intelligence & future warfare: Implications for international security. *Defense & Security Analysis, 35*, 1-23. https://doi.org/10.1080/14751798.2019.1600800.
32. Johnson, J. (2023). Automating the OODA loop in the age of intelligent machines: Reaffirming the role of humans in command-and-control decision-making in the digital age. *Defence Studies, 23*(1), 43-67. https://doi.org/10.1080/14702436.2022.2102486.
33. Jovičić, R., Gostimirović, L., & Milašinović, S. (2024). Use of New Technologies in the Field of Protection and Rescue During Disasters. *International Journal of Disaster Risk Management*, *6*(1), 111–122.
34. Kachanov, S. (2021). Methodology for Building Automated Systems for Monitoring Engineering (Load-Bearing) Structures, and Natural Hazards to Ensure Comprehensive Safety of Buildings and Constructions. International Journal of Disaster Risk Management (IJDRM), 3(2), 1-10.
35. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804.

36. LibreTexts. (2024, March 22). *Types of attacks*. Retrieved March 22, 2024, from https://eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.4_Attacks_-_Types_of_Attacks.
37. Manjak, M. M., & Miletić, S. M. (2011). Predlog koncepta komandno-informacionog sistema brigade KoV Vojske Srbije. *Vojnotehnički glasnik, 59*(2), 78-93. https://doi.org/10.5937/vojtehg1102078M.
38. Mayer, M. (2023). Trusting machine intelligence: Artificial intelligence and human-autonomy teaming in military operations. *Defense & Security Analysis, 39*(4), 521-538. https://doi.org/10.1080/14751798.2023.2264070.
39. Meerveld, H. W., Lindelauf, R. H. A., Postma, E. O., et al. (2023). The irresponsibility of not using AI in the military. *Ethics and Information Technology, 25*, 14. https://doi.org/10.1007/s10676-023-09683-0.
40. Military Africa. (2023, November). Artificial intelligence in the military. Retrieved March 22, 2024, from https://www.military.africa/2023/11/artificial-intelligence-in-the-military/.
41. Musman, S., Temin, A., Tanner, M., Fox, D., & Pridemore, B. (2010). Evaluating the impact of cyber attacks on missions.
42. Nedejkovic, S. (2015). *Evropska strategija bezbednosti i sajber pretnje - znala za Srbiju*. Beograd: Vojno delo. https://doi.org/10.5937/vojdelo.
43. Nikolić, N., Cvetković, V., Ivanov, A. (2023). Human resource management in environmental security. Belgrade: Scientific-Professional Society for Disaster Risk Management.
44. Ostojić, M., Karavidic, Z., & Projovic, D. (2017). Uticaj doktrine i koncepata na razvoj sposobnosti Vojske Srbije. *Vojno delo, 69*, 321-340. https://doi.org/10.5937/vojdelo17083210.
45. Payne, K. (2018). Artificial intelligence: A revolution in strategic affairs? Survival, 60(5), 7-32. https://doi.org/10.1080/00396338.2018.1518374.
46. Pirani Risk. (2024, March 16). *Artificial intelligence to combat cyber attacks*. Retrieved March 16, 2024, from https://www.piranirisk.com/blog/artificial-intelligence-to-combat-cyber-attacks.
47. RAND Corporation. (2022, November). *Ukraine's lessons for the future of hybrid warfare*. Retrieved March 16, 2024, from https://www.rand.org/pubs/commentary/2022/11/ukraines-lessons-for-the-future-of-hybrid-warfare.html.
48. RAND Corporation. (n.d.). *Reprints: RP223*. Retrieved March 22, 2024, from https://www.rand.org/pubs/reprints/RP223.html.
49. Sanz-Caballero, S. (2023). The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanities and Social Sciences Communications, 10*, 360. https://doi.org/10.1057/s41599-023-01864-y.
50. Scharre, P. (2016). Assessing and managing the risks of autonomous weapons. In *Autonomous Weapons and Operational Risk: Ethical Autonomy Project* (pp. 49–52). Center for a New American Security. http://www.jstor.org/stable/resrep06321.12.
51. Schraagen, J. M. (2023). Responsible use of AI in military systems: Prospects and challenges. *Ergonomics, 66*, 10.1080/00140139.2023.2278394.
52. SDI. (2024). The most useful military applications of AI. Retrieved March 22, 2024, from https://sdi.ai/blog/the-most-useful-military-applications-of-ai/#:~:text=Generative%20AI's%20analysis%2C%20scenario%20generation,to%20help%20predict%20future%20attacks.
53. Singh, S., Singh, M., & Singh, D. (2011). A survey on network security and attack defense mechanism for wireless sensor networks. *1*.
54. U.S. Department of Defense. (n.d.). *Joint Publication (JP) 3-12, Joint Cyberspace Operations*. Retrieved March 21, 2024, from https://irp.fas.org/doddir/dod/jp3_12.pdf.
55. U.S. Government Accountability Office (GAO). (n.d.). *U.S. less prepared to fight cybercrime than it could be*. Retrieved March 22, 2024, from https://www.gao.gov/blog/u.s.-less-prepared-fight-cybercrime-it-could-be.

56. Usai, A., Fiano, F., Messeni Petruzzelli, A., Paoloni, P., Farina Briamonte, M., & Orlando, B. (2021). Unveiling the impact of the adoption of digital technologies on firms' innovation performance. *Journal of Business Research, 133*, 327-336.
57. Vuletić, D. (2017). *Upotreba sajber prostora u kontekstu hibridnog ratovanja*. Beograd: Vojno delo. https://doi.org/10.5937/vojdelo1707308V.
58. Weick, K. E., & Sutcliffe, K. M. (2015). *Managing the unexpected: Sustained performance in a complex world* (3rd ed.). Jossey-Bass.

**Editor-in-Chief**

**Prof. Dr. Vladimir M. Cvetković**

## Biography

Prof. Dr. Vladimir M. Cvetković is recognized as a leading expert in Disaster Risk Management, with a focus on Risk Reduction, Preparedness, Response, and Recovery. He distinguishes himself as an esteemed Associate Professor specializing in Disaster Risk Management at the University of Belgrade, Faculty of Security, Department for Disaster Management and Environmental Security (Univerzitet u Beogradu, Fakultet bezbednosti). He (visiting professor) is a member of the Safety and Disaster Studies (SDS) working group at the Montanuniversität Leoben (https://www.sds-uni-leoben.at/arbeitsgruppe-sds/). With an illustrious career spanning over 15 years, he has dedicated his scholarly efforts to advancing the understanding and management of disasters. Dr. Cvetković's academic contributions are extensive, comprising a rich portfolio of over 300 research papers and 30 scientific monographs.

As a visionary leader in his field, Prof. Dr. Cvetković is renowned for founding significant initiatives such as the Scientific Professional Society for Disaster Risk Management in Serbia and the esteemed International Institute for Disaster Research. He also holds the distinguished position of Editor-in-Chief of the International Journal of Disaster Risk Management, exemplifying his influential role in shaping discourse and fostering collaboration within the academic community.

His doctoral thesis, titled "Citizens preparedness for responding to natural disaster caused by flood in Serbia," underscores his commitment to addressing real-world challenges in disaster management. Educationally, Prof. Dr. Cvetković's journey is marked by excellence. He completed his Undergraduate Studies in Criminalistic at the Academy of Criminal Investigation and Police Studies, Belgrade, graduating with a perfect GPA in 2010. Continuing his academic pursuit, he attained Postgraduate Studies in Criminalistic (2010-2012) and earned his PhD in Security, specializing in disaster risk management, from the University of Belgrade, Faculty of Security Studies (2012-2015).

Throughout his distinguished academic career, Prof. Dr. Cvetković has held various esteemed positions, including Assistant Professor at the University of Belgrade, Faculty of Security Studies (2017-present), where he imparts knowledge on disaster risk management and related subjects. Prior to this, he served as a Professor Assistant at the Academy of Criminal Investigation and Police Studies, Belgrade (2013-2017), and as a Teaching Associate (2011-2013) at the same institution, where he influenced and inspired future generations of scholars and practitioners.

Prof. Dr. Cvetković's impact extends beyond academia, as evidenced by his prolific research output and engagement in scholarly activities. He has reviewed over 200 scientific papers in national and international journals and proceedings, significantly advancing knowledge in his field. Additionally, he has actively participated in over 100 national and international scientific conferences, further solidifying his reputation as a thought leader and expert in disaster risk management.

His exemplary contributions have not gone unnoticed, as Prof. Dr. Cvetković has been honored with numerous awards and accolades throughout his career. Notably, he received the prestigious

Danubius Young Scientist Award for 2017, recognizing his extraordinary achievements in scientific activity and output. Furthermore, he has been the recipient of scholarships and awards for academic excellence, underscoring his dedication and scholarly prowess.

Prof. Dr. Vladimir M. Cvetković's multifaceted contributions, spanning academia, research, and leadership, reflect his unwavering commitment to advancing the field of disaster risk management. His pioneering initiatives and scholarly endeavors continue to shape discourse and drive innovation in addressing complex challenges posed by disasters globally.

MONTAN UNIVERSITÄT LEOBEN

SDS SAFETY AND DISASTER STUDIES

PANK-Postgraduate, extra occupational master study, 4 semesters
PANK-Academic, extra occupational expert training, 3 semesters

■ interdisciplinary ■ research-guided ■ practice-oriented