HOW INFORMATION SYSTEMS ARE RESHAPING NATIONAL SECURITY STRATEGIES

Associate Professor Florentina Loredana DRAGOMIR, PhD
"Carol I" National Defence University
DOI: 10.55535/RMT.2025.1.10

Information systems play a key role in modern national security strategies, providing advanced tools for threat management and strategic decision-making. The rapid flow of information influences the geopolitical balance, and the effective use of information technology has become a priority for governments and security institutions. As real-time access to data has increased, as the ability to analyze massive volumes of information and automate the decision-making process fundamentally transforms the way the state protects national interests, advanced technologies are integrated into national security systems. Also, the increase in interconnectivity between different security services and government institutions leads to the creation of interoperability and reaction time in emergency situations. The article presents an analysis of how information systems influence national security strategies, highlighting both their benefits and the challenges they generate.

Keywords: interoperability; information warfare; artificial intelligence; information systems; human rights;

INTRODUCTION

Technology offers a significant advantage in data collection and analysis, allowing for the anticipation and neutralization of threats before they manifest themselves. However, with this increased dependence on technology, there are also risks related to cybersecurity, information protection, and the misuse of sensitive data, which determine the development of appropriate policies and regulations that ensure the balance between security and respect for fundamental human rights.

Information systems represent an essential pillar in modern national security strategies, providing innovative solutions to protect the interests of states and citizens. They are in a constant adaptation with the development of security infrastructures and mechanisms, allowing for international collaboration in this area. Investments in technology, the development of analytical capabilities and the strengthening of data protection are fundamental aspects for ensuring effective national security in this century. The lack of a rapid and efficient exchange of information can lead to delays in making critical decisions and to an insufficient response to crises. Therefore, states are increasingly investing in the development of information infrastructures that allow for the secure sharing of data between defence, intelligence and law enforcement institutions. Models for integrating information systems differ depending on the structure of each state and the level of international cooperation. In many countries, national security depends on integrated networks that connect command and control centres, intelligence agencies and military structures for effective coordination. In the same spectrum, internationally, strategic alliances such as NATO, and partnerships between intelligence agencies allow for the rapid exchange of information and real-time analysis of threats. The implementation of common data platforms and the use of artificial

Investments in technology, the development of analytical capabilities and the strengthening of data protection are fundamental aspects for ensuring effective national security in this century. The lack of a rapid and efficient exchange of information can lead to delays in making critical decisions and to an insufficient response to crises.

intelligence to correlate and interpret information are becoming the used solutions to increase the response capacity of states. International standards such as those developed by the United Nations, the European Union or NATO play a crucial role in ensuring interoperability between the security systems of different states. Although these standards are concisely defined, the challenges remain significant, especially due to technological, political and legal differences. The lack of a unified regulatory framework for information exchange as well as the concerns about data protection and national sovereignty can make system integration difficult. Technological vulnerabilities and risks associated with cybersecurity also represent major obstacles to creating secure and efficient information infrastructures. Establishing common standards, developing secure information exchange platforms and adopting the latest technologies are necessary steps for effective defence against emerging threats.

Modern interoperability models involve the creation of common platforms where data can be securely accessed by relevant agencies, while respecting the rules on the protection of sensitive information.

INTEGRATION AND INTEROPERABILITY OF INFORMATION SYSTEMS IN NATIONAL AND INTERNATIONAL SECURITY

Modern national security can no longer operate in isolation, but depends on a complex network of collaboration between domestic agencies and international partners. Threats are increasingly diverse and unpredictable, and rapid information exchange is crucial for crisis prevention and management. From combating terrorism and organized crime to managing natural disasters, effective integration of information systems allows for better coordination and a faster response to security challenges.

A key aspect of this integration is the connection of information systems used by defence, intelligence, and law enforcement institutions. In many countries, these entities operate on separate infrastructures, which can make data exchange difficult and reduce reaction time. Modern interoperability models involve the creation of common platforms where data can be securely accessed by relevant agencies, while respecting the rules on the protection of sensitive information (Ahmad, Qureshi, 2023). International partnerships, such as those

within NATO or the European Union, have led to the implementation of common information networks that facilitate coordination between different security structures. Terrorism, organized crime, information warfare and hybrid conflicts require a rapid and secure exchange of information between security institutions from different states, and the lack of close collaboration can lead to operational gaps, delays in decision-making and failures in preventing major crises. As a consequence, one of the main reasons why international cooperation is crucial is the transnational typology of security threats (Dragomir, 2024). Terrorist groups and criminal networks do not operate within the borders of a single state, but use global infrastructures for financing, recruitment and coordination. Therefore, no national agency can manage these challenges alone and the exchange of information between security agencies from different countries allows for the early identification of threats, the prevention of attacks and the coordination of the response in crisis situations. Examples in this regard are international structures, such as Interpol and Europol, which facilitate cooperation between states in investigating and neutralizing common threats, providing a secure platform for sharing operational data. Another essential component of effective cooperation is the interoperability of information systems used by intelligence agencies. Therefore, many international alliances develop common secure networks for sharing classified information, such as the *"Five Eyes"* system (USA, UK, Canada, Australia, New Zealand) or NATO platforms for managing security data. Such infrastructures allow a real-time flow of information, facilitating strategic decision-making. In addition to data exchange, international cooperation also involves the development of common defence and security strategies. Military alliances and international security structures, such as NATO and the UN, promote joint exercises, crisis simulations and training programmes to ensure a coordinated response to global threats. For example, joint exercises on cyber defence and critical infrastructure security help member states improve their ability to react to hybrid and asymmetric attacks. Despite the obvious benefits of collaboration, there are also numerous challenges that need to be overcome, such as the lack of trust between states caused by political, historical and strategic differences.

ROMANIAN MILITARY THINKING

Terrorist groups and criminal networks do not operate within the borders of a single state, but use global infrastructures for financing, recruitment and coordination. Therefore, no national agency can manage these challenges alone and the exchange of information between security agencies from different countries allows for the early identification of threats, the prevention of attacks and the coordination of the response in crisis situations.

Some governments are reluctant to share sensitive information, fearing data leaks or its use for purposes that run counter to national interests. To overcome these obstacles, it is essential to create clear legal frameworks and procedures that regulate the exchange of information and its use exclusively for collective security purposes.

❖ **The Importance of Standardization and Common Protocols in Information Exchange**

Standardization and the use of common protocols in information exchange are essential for ensuring an efficient and coordinated national security environment. As threats evolve rapidly, the interoperability of information systems is crucial for the rapid and coordinated response of security agencies. Without clear standards, each institution or state could use different technologies and structures, which would create barriers to communication and slow down the decision-making process.

Within NATO, the use of unified standards for data transmission and storage allows for efficient coordination between member states, reducing the risk of errors caused by the incompatibility of national systems.

Whether it is law enforcement, intelligence services or defence structures, the use of common data formats and secure channels allows for rapid access to essential information. For example, within NATO, the use of unified standards for data transmission and storage allows for efficient coordination between member states, reducing the risk of errors caused by the incompatibility of national systems.

Another essential aspect of standardization is communications security. The lack of common protocols can lead to exploitable vulnerabilities by hostile actors, which compromises the integrity of transmitted data. By establishing international standards for encryption and authentication, sensitive information can be protected against cyberattacks and unauthorized interception. For example, the European Union and NATO implement security protocols based on advanced encryption and multi-factor authentication to prevent unauthorized access to classified information networks.

In addition to technical aspects, standardization also plays an important role in defining operational procedures for managing crises and emergencies. There are clear rules on how information should be shared and analysed. That is why many international organizations

have developed guidelines and standard procedures for responding to terrorist threats, hybrid attacks or natural disasters. These frameworks of action allow for a faster and more effective response to events with an impact on national security.

Despite the obvious advantages, the standardization process faces numerous challenges, especially due to the differences between national policies and strategic interests of each state. Some countries are reluctant to adopt common protocols for fear of losing control over their own security infrastructures. Also, the integration of international standards requires significant investments in the modernization of existing infrastructure and in the training of personnel who manage information systems. In addition to these aspects, cybersecurity plays a critical role, as any vulnerability in an interconnected system can be exploited by hostile actors to compromise information networks. In the future, the development of information infrastructures for security must follow directions that maximize the efficiency and security of data exchange. The use of artificial intelligence and machine learning to analyse large volumes of information can considerably improve the response capacity of security agencies. Also, the development of quantum communications and advanced encryption technologies will allow for more effective protection of sensitive data. Standardization and the use of common protocols in the exchange of information are fundamental to strengthening national and international security. They facilitate effective communication between agencies, reduce the risks associated with technological vulnerabilities, and allow for a rapid response in crisis situations. Although their implementation can be a complex and costly process, the long-term benefits far outweigh the challenges, contributing to the creation of a more robust security environment that is more adaptable to the challenges of the future.

ROMANIAN MILITARY THINKING

The development of quantum communications and advanced encryption technologies will allow for more effective protection of sensitive data.

Standardization and the use of common protocols in the exchange of information are fundamental to strengthening national and international security.

❖ **Technological and Legal Challenges in Ensuring Interoperability**

Interoperability of information systems is essential for national security, but the implementation process faces multiple challenges, both technologically and legally. As states and international institutions

try to create integrated networks for information exchange, they face difficulties related to the compatibility of existing infrastructures, the protection of sensitive data and legislative differences. These challenges must be addressed to enable an efficient and secure exchange of information between security agencies and international partners.

From a technological point of view, one of the biggest problems is the lack of a homogeneous infrastructure. Many government agencies and security structures use information systems developed at different times, with varying technologies, which makes it difficult to integrate them into a common framework. Some of these systems are not compatible with modern platforms, which makes it difficult to exchange information in real time. Also, the use of different data storage and processing architectures can lead to inconsistencies in the interpretation of information, affecting decision-making ability.

In the European Union, the General Data Protection Regulation (GDPR) imposes strict restrictions on the transfer of data to third countries, which can complicate the exchange of information with states that do not comply with the same standards.

Another technological challenge is ensuring the cybersecurity of interconnected systems. When multiple agencies or states share information over common networks, the risk of this data being intercepted or compromised increases exponentially. Security infrastructures must be robust enough to prevent cyberattacks, and encryption and authentication protocols must be standardized to ensure data protection. However, some states are reluctant to adopt common technological solutions, fearing of the potential vulnerabilities that could be exploited by hostile actors.

From a legal perspective, legislative differences between states represent a major obstacle to ensuring interoperability. Each country has its own regulations on data protection, access to classified information, and individual rights of citizens. These differences can make it difficult to share information between partners, as national legislation may prohibit the transmission of certain types of data to external entities. For example, in the European Union, the General Data Protection Regulation (GDPR) imposes strict restrictions on the transfer of data to third countries, which can complicate the exchange of information with states that do not comply with the same standards.

Another legal issue is related to national sovereignty and control over strategic information. Many states believe that information sharing within international networks could reduce national autonomy in managing internal security. Therefore, they hesitate to participate in extended interoperability initiatives or impose strict limits on the type of information that can be shared. This lack of trust can slow down the implementation of effective interoperability solutions and create gaps in collective security, causing states to adopt different approaches, which complicates the integration of networks. In the absence of formal agreements on the use and protection of shared information, there is a risk that data transmitted between partners will be misused or exposed to external threats. To overcome these challenges, extensive cooperation between states and security agencies is needed, in terms of both modernizing technological infrastructures and harmonizing the legislative framework. The development of international standards that are accepted by all parties involved could facilitate information sharing and reduce the risks associated with interoperability. Also, the creation of mechanisms for verifying and auditing the security of systems could strengthen trust between partners and allow for a more efficient integration of information networks in the field of national and international security.

The development of international standards that are accepted by all parties involved could facilitate information sharing and reduce the risks associated with interoperability. The creation of mechanisms for verifying and auditing the security of systems could strengthen trust between partners and allow for a more efficient integration of information networks in the field of national and international security.

Another challenge is represented by the legislative differences in terms of data protection and electronic surveillance. In the European Union, for example, the GDPR imposes strict restrictions on the collection and use of personal information, which can complicate cooperation with states that do not comply with the same privacy standards. Here too, it is necessary to harmonize national legislation to allow for an efficient exchange of information, without compromising the rights and freedoms of citizens. Investments in common security infrastructures and the creation of clear legal frameworks are essential for strengthening this collaboration and for effectively adapting to all the challenges of the future.

INFORMATION WARFARE AND AI TECHNOLOGIES USED

Information warfare has become an essential component of state security strategies, in an increasingly interconnected and technology-dependent global context. This type of conflict takes place in cyberspace and digital environments, covering a wide range of information manipulation techniques. Information warfare involves the use of information to influence the perceptions and behaviours of individuals, groups or entire nations, with the aim of destabilizing, weakening the authority of governments or manipulating public opinion in favour of a certain strategic interest.

Information warfare involves the use of information to influence the perceptions and behaviours of individuals, groups or entire nations, with the aim of destabilizing, weakening the authority of governments or manipulating public opinion in favour of a certain strategic interest.

Essentially, information warfare involves control over the flow of information and statements that are transmitted to the public. One of the fundamental tools of this type of warfare is disinformation that aims to mislead the audience (Dragomir-Constantin, 2025-a). This process can be extremely effective when carried out in a crisis context, where the public is more vulnerable and more prone to accepting incorrect information, often out of a desire to quickly understand a complex situation. Disinformation can be widely applied through traditional media channels, but especially through online social media platforms, which allow for the rapid spread and amplification of messages, often without their source being properly verified.

Another aspect of information warfare is digital propaganda (Dragomir-Constantin 2025-b). Unlike disinformation, which aims to mislead with false information, propaganda is based on the selection and manipulation of true information to support a particular political or ideological agenda. Digital propaganda uses modern means of communication to create a favourable narrative, which can mobilize masses of people, influence political elections, or destabilize regimes. In this sense, social networks are used not only to spread information, but also to create online communities that support certain points of view and actively work to promote them. For example, a propaganda message can be amplified through coordinated campaigns of fake accounts or botnets that contribute to creating an erroneous image of a political or social situation, making it appear more favourable to a certain group.

Psychological operations represent another method used in information warfare. They are coordinated activities aimed at influencing the perceptions, attitudes and behaviours of a target audience through the use of sophisticated information manipulation techniques. The aim is to induce a strong emotional reaction, which changes public opinion or destabilizes certain social or political groups. In the modern context, artificial intelligence (AI) technologies play a central role in the development of these operations (Zhang, Wang, 2023). AI allows the processing of an enormous volume of data to identify the psychological vulnerabilities of the target population and to personalize messages based on the previous reactions and behaviours of users (Ib.). Thus, AI algorithms are able to create and disseminate messages that are adapted to the specific profile of each person, whether it is a news consumer or a voter. These personalization techniques are extremely effective in manipulating opinions and can have a significant impact on political choices, radicalization, or social polarization (Ngguyen, 2024).

AI allows the processing of an enormous volume of data to identify the psychological vulnerabilities of the target population and to personalize messages based on the previous reactions and behaviours of users.

In addition, AI technologies allow for the automation and expansion of influence operations, making them much faster and harder to detect. By using machine learning algorithms, malicious actors can analyse the behaviours and preferences of users on social media platforms, generating messages that resonate with their pre-existing beliefs and ideas. Thus, not only can information be controlled, but the public's reaction can also be anticipated, making information warfare much more effective and subtle. AI can also help create deepfakes – fake but convincing images and videos that can be used to discredit individuals or institutions, thus amplifying political or social conflicts.

In the face of these advanced techniques of information manipulation, states and international organizations must develop technological and legislative capacities to combat the negative effects of information warfare (Khraisat, Kanaan, 2023). Monitoring and regulating social media platforms, protecting personal data, and raising public awareness about the risks of disinformation are just some of the measures that can be implemented to protect modern societies. It is also essential that government agencies and the private sector should

collaborate to create technological infrastructures that allow for the rapid detection of manipulation campaigns and help counter them.

Information manipulation through disinformation, digital propaganda and psychological operations poses a serious threat to global political, social and economic stability. Countering these techniques is not only a matter of national security, but also a collective global responsibility. Efforts to protect information integrity must include not only the development of cyber defence technologies, but also public education on the risks of information manipulation, thus encouraging a more conscious and critical use of available information.

A deepfake could create a video of a political leader giving an inflammatory speech or making outrageously false statements, causing confusion and undermining public trust in political leaders or government institutions. This visual and auditory manipulation is often extremely difficult to detect by the human eye or even by traditional detection algorithms, making deepfakes a very effective tool in information warfare.

Artificial intelligence has evolved into an extremely powerful tool in information warfare, with the ability to rapidly create and disseminate fake information. One of the most worrying uses of AI in this context is the generation of fake content, such as deepfakes, manipulated images and videos, which can be used for large-scale disinformation. These technologies not only allow the creation of extremely realistic materials, but also rapidly amplify messages, often through social networks and other digital platforms, causing them to spread at a pace almost impossible to control. Deepfakes are a classic example of how AI can generate fake content that appears authentic. Using advanced machine learning techniques such as generative adversarial neural networks (GANs), AI can manipulate images and videos, altering key aspects of them, such as people's faces or voices, to make it appear that they said or did something they did not. A deepfake could create a video of a political leader giving an inflammatory speech or making outrageously false statements, causing confusion and undermining public trust in political leaders or government institutions. This visual and auditory manipulation is often extremely difficult to detect by the human eye or even by traditional detection algorithms, making deepfakes a very effective tool in information warfare.

Another type of fake content created through AI is the generation of manipulated images and photos, which are used to support false narratives or to create the impression of an event that never happened. For example, during a conflict or political crisis, fake images can be created to show a violent event or atrocity that did not happen,

which can fuel panic, hatred, and violence. These images can be manipulated to include false details, such as non-existent weapons, fabricated victims, or altered locations, thereby contributing to distorting reality and influencing public opinion in a harmful way.

Fake videos, in addition to deepfakes, are another form of AI-generated content. These can include fake interviews, recordings of conversations between political leaders or military officers, or even private conversations between citizens that are manipulated to create the impression of misconduct or conspiracy. AI can also be used to modify existing video sequences, removing or adding elements to change the context or original message. For example, a video can be cut and edited to create a statement that supports a particular ideology, which can affect both a person's public image and the political stability of a state. One of the most dangerous aspects of AI-generated fake content is that this type of information not only spreads quickly, but can also penetrate deeply into the collective consciousness. As people have constant access to information via the internet, it is increasingly difficult for individuals to discern between truth and lies, especially when the fakery is carried out at an extremely sophisticated level. AI technologies can also create fake content continuously, so that information warfare becomes almost a constant battle between those who create it and those who try to detect it. In this race, detecting deepfakes and other types of fake content becomes a huge challenge, and traditional cybersecurity and information verification systems are not always fast enough to counteract their effects.

ROMANIAN MILITARY THINKING

AI technologies can create fake content continuously, so that information warfare becomes almost a constant battle between those who create it and those who try to detect it. In this race, detecting deepfakes and other types of fake content becomes a huge challenge, and traditional cybersecurity and information verification systems are not always fast enough to counteract their effects.

To combat these threats, a concerted effort is needed between governments, international organizations, and technology companies to develop advanced solutions to detect deepfakes and other forms of fake content.

Propaganda automation, through the use of bots and algorithms to amplify messages and influence public opinion, is also a key component of modern information warfare.

Sentiment analysis and manipulation with AI algorithms that analyse users' emotions and behaviours to tailor propaganda messages allow to decipher not only the words used by users,

but also the tone, context, and emotions behind them. These algorithms can identify psychological traits of individuals, such as fear, anger, pride, or sadness, and adapt the content conveyed to stimulate or modify these reactions. For example, algorithms can detect a state of frustration or fear in online posts and target messages that amplify those feelings, thereby leading the user to a desired behaviour or reaction. An example of sentiment manipulation through AI analysis can be seen in disinformation campaigns aimed at creating panic or encouraging hatred in a particular social or political context. In these cases, messages are tailored to exploit the emotional vulnerabilities of a population, provoking a stronger visceral reaction than a simple presentation of factual information. For example, during international crises or conflicts, algorithms can distribute messages that exaggerate dangers, reinforcing the feeling of insecurity and collective anxiety. These tactics can lead to the creation of a climate of panic and fear, which makes individuals and groups more susceptible to manipulation and less willing to seek alternative sources of information. Moreover, AI can tailor propaganda messages to influence specific user behaviours, including their electoral choice or support for political actions. Algorithms are able to identify and exploit users' cognitive biases, providing them with messages that align with their existing beliefs, and amplifying and channelling them in a desired direction. This phenomenon is known as the *"digital echo chamber"*, where users are only exposed to information that confirms their opinions, and AI amplifies this cycle by recommending messages that maximize the emotional impact on users. In addition to sentiment analysis, algorithms can also learn complex behavioural patterns, with the ability to predict user reactions under certain conditions and adapt messages accordingly. For example, an AI algorithm can identify a user who is prone to responding to hateful or fear-based messages and create a message that responds to these behavioural traits, thereby increasing the effectiveness of the manipulation campaign. This type of extreme message personalization makes propaganda much more subtle and difficult to detect, which makes it even more dangerous for social stability and cohesion. The impact of this technology

An example of sentiment manipulation through AI analysis can be seen in disinformation campaigns aimed at creating panic or encouraging hatred in a particular social or political context. In these cases, messages are tailored to exploit the emotional vulnerabilities of a population, provoking a stronger visceral reaction than a simple presentation of factual information.

on national security is significant. The manipulation of public sentiment and behaviour can destabilize political institutions, divide society, and undermine trust in government and fundamental state institutions. Moreover, the use of AI to manipulate collective emotions can lead to extreme polarization of public opinion and a radicalization of social and political behaviours. It can create a climate conducive to extremism and internal conflict, facilitating external interference and undermining national stability. To combat these threats, it is essential that governments and international institutions should collaborate to develop regulations and technologies that monitor and prevent emotional manipulation in information warfare. It is also necessary for citizens to be educated to recognize AI-based manipulation tactics and to develop critical thinking skills, in order to be able to identify and reject messages that are not only false, but also strategic in emotionally influencing their behaviour.

In conclusion, the use of AI to analyse and manipulate sentiment represents an extremely sophisticated form of information warfare, with a considerable impact on national security. This technology offers the possibility of influencing opinions and behaviour in a much more effective and subtle way than traditional propaganda methods, which makes protection against it a priority for any state that wants to defend its democracy and social cohesion. This form of manipulation can target both the individual and the masses, and the effects can be devastating for social cohesion, political stability and national security. The impact of information systems on national security strategies is undeniable. They have revolutionized the way states respond to global threats, but they have also brought new challenges that require constant attention. Investments in the protection of these systems must be continuous, and technological development must go hand in hand with respect for the fundamental principles of democracy and human rights. Only in this way can we build a future in which national security and innovation coexist harmoniously, protecting both the state and its citizens.

The impact of information systems on national security strategies is undeniable. They have revolutionized the way states respond to global threats, but they have also brought new challenges that require constant attention.

CONCLUSIONS

Information systems have become an indispensable component of national security strategies, revolutionizing the way governments identify and manage threats. Real-time access to relevant data and the ability to analyse massive volumes of information allow for more effective risk anticipation, increasing the ability of states to respond quickly and in a coordinated manner to emerging challenges.

Another major benefit is the interconnectivity between security institutions, which improves interoperability and optimizes decision-making processes. Automation and integration of advanced technologies into security infrastructures facilitate not only rapid response to crises, but also the development of better-founded preventive policies. However, the digitalization of national security comes with significant challenges, such as cyber risks, vulnerabilities in critical infrastructures, and ethical dilemmas regarding surveillance and data protection. The successful implementation of these systems depends on the balance between technological innovation, appropriate regulation and adaptable security strategies. Information systems are not only transforming traditional methods of defence and security, but also redefining geopolitical relations and the way in which states protect their interests. The effective management of these technologies will be a decisive factor in maintaining national and international stability and security. The future of national security will depend not only on technological advances, but also on the ability of decision-makers to integrate innovations in a responsible, sustainable and strategic manner.

The interconnectivity between security institutions improves interoperability and optimizes decision-making processes. Automation and integration of advanced technologies into security infrastructures facilitate not only rapid response to crises, but also the development of better-founded preventive policies.

BIBLIOGRAPHY:

1. Ahmad, S., Qureshi, M. (2023). *An analysis of cloud security frameworks, problems and proposed solutions*. Network, 3(3), 422-450, https://doi.org/10.3390/network3030045, retrieved on 2 February 2025.
2. Dragomir, F.L. (2024). *The potential for intensifying Austria's opposition to Schengen Enlargement*. In *European Journal of Accounting, Finance & Business*, 12(2), fromhttps://accountingmanagement.ro/index.php?pag=showarticle&issue=35&year=2024&brief=3516, retrieved on 22 January 2025.

3. Dragomir-Constantin, F.-L. (2025-a). *Thinking Patterns in Decision-Making in Information Systems*. New Trends in Psychology, 7(1), pp. 89-98, https://dj.univ-danubius.ro/index.php/NTP/article/view/3255, retrieved on 22 January 2025.
4. Dragomir-Constantin, F.-L. (2025-b). *Thinking Traps: How High-Performance Information Systems Correct Cognitive Biases in Decision-Making.* New Trends in Psychology, 7(1), pp. 99-108, https://dj.univ-danubius.ro/index.php/NTP/article/view/3257, retrieved on 2 February 2025.
5. Khraisat, A., Kanaan, M. (2023). *A comprehensive review of cyber security vulnerabilities, threats, and attacks in cloud computing*. Electronics, 12(6), 1333, https://doi.org/10.3390/electronics12061333, retrieved on 23 February 2025.
6. Nguyen, H.T., Nguyen, V.T. (2024). *Artificial intelligence in cybersecurity: A review and a case study*. Applied Sciences, 14(22), 10487, https://doi.org/10.3390/app142210487, retrieved on 2 February 2025.
7. Zhang, L., Xu, J. (2023). *A critical cybersecurity analysis and future research directions for the Internet of Things (IoT)*. Sensors, 23(8), 4117, https://doi.org/10.3390/s23084117, retrieved on 2 February 2025.
8. Zhang, Y., Wang, F. (2023). *A comprehensive framework for cyber behavioural analysis based on a hybrid approach*. Applied System Innovation, 3(3), 32, https://doi.org/10.3390/asi3030032, retrieved on 2 February 2025.