ISSN 2421-4442

SICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

INTERNATIONAL JOURNAL - Italian Team for Security, Terroristic Issues & Managing Emergencies

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

INTERNATIONAL JOURNAL
Italian Team for Security,
Terroristic Issues & Managing Emergencies

20

ISSUE 2/2024

Milano 2024

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SICUREZZA, TERRORISMO E SOCIETÀ
INTERNATIONAL JOURNAL – Italian Team for Security, Terroristic Issues & Managing Emergencies

ISSUE 2 – 20/2024

Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)
web: www.educatt.it/libri

Associato all'AIE – Associazione Italiana Editori

ISSN: 2421-4442
ISSN DIGITALE: 2533-0659
ISBN: 979-12-5535-352-2

copertina: progetto grafico Studio Editoriale EDUCatt

Sommario

TERRORISM, WARFARE, INTELLIGENCE, STRATEGIC COMMUNICATION, CRISIS MANAGEMENT AND TECHNOLOGICAL ADVANCEMENTS AT THE CROSSROAD

The Potential Use of Artificial Intelligence in Crisis Management

Krzysztof Kaczmarek, Mirosław Karpiuk, Urszula Soler

Krzysztof Kaczmarek[1] Ph.D. in Social Sciences in the discipline of political science and administration. Currently, he works at the Koszalin University of Technology, Faculty of Humanities, Department of Regional and European Studies. He specialises in issues related to hybrid threats, including cybersecurity, disinformation, and critical infrastructure protection.

Mirosław Karpiuk[2] professor of social sciences in the discipline of legal sciences. Currently employed at the University of Warmia and Mazury in Olsztyn, at the Faculty of Law and Administration, Department of Administrative Law and Security Sciences. He specialises in issues related to security and defence, including the administration of security and public order or cybersecurity.

Urszula Soler[3] is graduated in polish literature, social philosophy and sociology. She is Assistant Professor at the John Paul II Catholic University of Lublin. She is specialized in disposition groups of the military social system. Her research interests are focused on security, paramilitary organizations, food security, technology assessment, sustainable development and innovations. She is founding member of the PANTA (Polish Academic Network of Technology Assessment) and founder of Polish Academic Legion; cooperates also for many years with Catholic University of Sacred Heart (Milan).

Abstract

This article focuses on the application of artificial intelligence (AI) in crisis management, taking into account both the legal and practical aspects. In the circumstances of growing challenges related to crisis management, AI is emerging as a key tool enabling high-speed big data analysis and decision-making processes. The author discusses how AI might contribute to better prediction, monitoring and response in emergencies, including natural and man-made disasters. Emphasis is also placed on the ethical and legal aspects of AI, including the need to develop a regulatory framework and to take into account accountability and transparency

[1] PhD, Koszalin University of Technology, Faculty of Humanities, Eugeniusza Kwiatkowskiego 6e, 75-343 Koszalin, Poland, ORCID: https://orcid.org/0000-0001-8519-1667 Corresponding author e-mail: puola@tlen.pl.
[2] Prof., PhD, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Dybowskiego 13, 10-723 Olsztyn, Poland ORCID: https://orcid.org/0000-0001-7012-8999 Corresponding author e-mail: miroslaw.karpiuk@uwm.edu.pl.
[3] Assoc. Prof., PhD, The John Paul II Catholic University of Lublin, Institute of Political Science and Public Administration, Al. Racławickie 14, 20-950 Lublin, Poland ORCID: 0000-0001-7868-8261 Corresponding author e-mail: urszula.soler@kul.pl.

principles. The paper sheds light on the limitations of AI, indicating the need for continued supervision and algorithm updates, and points to the potential risks resulting from errors in algorithms and unconscious bias. In the context of crisis management, the role of AI in counteracting disinformation that might trigger or escalate emergencies has also been discussed. The author of the paper stresses that, despite the enormous potential of AI, its effective application in crisis management requires a responsible approach, taking into account the ethical, legal, and social aspects.

Questo articolo si concentra sull'applicazione dell'intelligenza artificiale (IA) nella gestione delle crisi, prendendo in considerazione sia gli aspetti legali che quelli pratici. In un contesto di sfide crescenti legate alla gestione delle crisi, l'IA sta emergendo come uno strumento chiave che consente di analizzare ad elevata velocità i big data e i processi decisionali. L'autore discute come l'IA possa contribuire a migliorare la previsione, il monitoraggio e la risposta alle emergenze, compresi i disastri naturali e quelli causati dall'uomo. Viene posto l'accento anche sugli aspetti etici e legali dell'IA, compresa la necessità di sviluppare un quadro normativo e di tenere conto dei principi di responsabilità e trasparenza. Il contributo fa luce sui limiti dell'IA, indicando la necessità di una supervisione continua e di aggiornamento degli algoritmi, e sottolinea i potenziali rischi derivanti da errori negli algoritmi e da pregiudizi inconsci. Nel contesto della gestione delle crisi, è stato discusso anche il ruolo dell'IA nel contrastare la disinformazione che potrebbe scatenare o aggravare le emergenze. L'autore dell'articolo sottolinea che, nonostante l'enorme potenziale dell'IA, la sua applicazione efficace nella gestione delle crisi richiede un approccio responsabile, che tenga conto degli aspetti etici, legali e sociali.

Keywords

Artificial intelligence, big data, crisis management, data analysis, decision-making algorithms

1. Introduction

Technological progress, the growing computing power of digital tools, and the emergence of new ones contribute to transforming how individuals, societies and states function. A substantial part of such operations has been moved to the Internet, and algorithms control an increasing share of human activity. This refers to both the private and professional life and social interactions. Artificial intelligence is the most advanced among all the currently available digital tools. However, we should remember that AI is evolving, expanding the range of its potential applications.

The algorithms that form part of AI can make autonomous decisions based on big data analysis, self-correct errors and make decisions based on previous experience. Given that, it can be used where it is necessary to rapidly analyse information and identify patterns and interdependencies. This allows AI to find optimum solutions to a given problem in an incomparably shorter time than it would be needed for a human to complete. Therefore, AI might find specified applications in crisis management.

The literature on the subject does not provide a single, widely applied and accepted definition of an emergency and crisis (Walas-Trębacz, Ziarko 2011, p. 19). However, for the purpose of this paper, it has been assumed that an emergency is a set of circumstances that disrupt the normal functioning of a system in a sudden way (Walas-Trębacz, Ziarko 2011, p. 23). As per Article 3 (1) of the Polish Crisis Management Act of 26 April 2007 (consolidated text, Journal of Laws of 2023, Item 122), an emergency situation is understood as circumstances which have a negative impact on the level of security of the population, property of significant size, or the natural environment and result in substantial limitations of the activities performed by public administration authorities due to insufficient forces and resources.

The use of the opportunities that AI provides allows us to predict the occurrence of an emergency and provides the possibility to prepare appropriate forces and resources for adverse circumstances. It is also important to note that the analysis of large quantities of information and data allows the identification of patterns that a human is most often unable to notice, given especially that the rapidly changing surroundings result in the occurrence of new factors or in the increased probability that the factors which have previously been highly unlikely will occur. In crisis management, it is worth remembering that unlikely events are not impossible (Kaczmarek, 2023, p. 78). It is particularly crucial at the prediction and preparation stages. Unlike humans, AI can predict such situations.

However, the opportunities that AI creates in crisis management will not guarantee that they will be used effectively. In this context, it is critical to ensure that persons using digital tools have the appropriate skills to do so. It should also be noted that current AI technology is not the peak achievement in this sphere and is still evolving. Moreover, it is a man-made algorithm that might contain errors that have not been identified. Given that, the decisions it makes may also be faulty. However, such deficiencies are most often the outcome of the user's error, not the system. They might result from the user's incorrectly interpreting or ignoring analysis results.

Artificial intelligence has the potential to bring multiple benefits to people, both in the social and economic spheres. It is becoming an increasingly important tool in the operations of public and private entities. On the one hand, artificial intelligence tools are aimed at accelerating and streamlining decision-making processes or allowing the personalisation of products and services to tailor them to individual needs. On the other hand, the data being collected at a large scale, which is necessary for the proper operation of artificial intelligence, and automated decision-making processes, always pose a risk of infringing specified human rights and liberties, both at the algorithm design stage and at the AI functioning stage (Kostrubiec 2021, p. 37).

2. Limitations of AI

In the context of crisis management, it is imperative to understand the limitations of AI, and the need for continued supervision and algorithm updates. The monitoring of, and response to, the rapidly changing conditions of natural disasters may be a good example here. AI may provide data on changes in the environment. However, the final decision on evacuation or other preventive measures should be made by experienced experts who can assess the social or political context. Integrating data from various sources and systems is one of the key challenges related to using AI in crisis management. The multitude of data formats, communication protocols and security levels might hinder the effective coordination of actions. Therefore, it is essential to develop standards and protocols allowing seamless information exchange between entities and systems.

Furthermore, emphasis should be placed on the ethical and legal aspects of using AI in crisis management. Decisions made by AI could have far-reaching consequences for individuals, societies and states. For that reason, it is essential to take into account the principles of accountability, transparency and respect for human rights in designing and implementing AI algorithms. In the legal context, it is necessary to create a regulatory framework that will specify the entities accountable for decisions made by AI. This includes issues related to the responsibility for algorithm errors, personal data protection and compliance with local and international laws. Special attention should also be paid to cybersecurity, defined as the capacity of information networks and systems to maintain proper operation capabilities (Kostrubiec 2022, p. 28).

In a digital state, information and communication (ICT) systems are particularly vital. They serve fast communication purposes and may also be used to provide services or perform certain tasks. They have a wide range of applications, from entertainment, through communication, education, and employment, to the assurance of digital security. From the perspective of the normal functioning of the state, it would be crucial to not only perform tasks with the use of cyberspace but also to ensure cybersecurity. Cyberspace must be protected continuously as the state uninterruptedly performs its tasks in times of crisis or conflicts (Bencsik, Karpiuk 2023, p. 83).

Cyberthreats can result in various negative phenomena. This might lead to a crisis, particularly if cyberattacks are targeted against ICT systems used by the state to fulfil its strategic objectives, including those related to the assurance of the uninterrupted operation of critical infrastructure. Threats in cyberspace might often give rise to an emergency, particularly if public institutions and private entities are, to a large extent, computerised, and the ICT systems they use are not always duly protected (Karpiuk 2022, p. 114). In the

event of states that rely on ICT systems in their operations, the interference in such systems might take the form of cyberattacks. Given the functioning of the state, and the public structures and private entities operating within its framework, it is crucial to ensure the efficient protection of critical infrastructure covering strategic sectors. The protection of such infrastructure consists of safeguarding ICT systems against cyberthreats (Czuryk 2023, p. 50). In addition, critical infrastructure can be duly protected by using artificial intelligence. With AI, it is not only possible to predict the risk of threats affecting the proper functioning of the infrastructure but also to eliminate them.

3. The application of artificial intelligence in counteracting the impact of natural disasters

Artificial intelligence plays a key part in combating the effects of natural disasters, offering a wide range of advanced options to choose from. Some of the main AI applications include early warning and prediction of disasters. AI systems may analyse big data sets from various sources, such as satellite data, weather data, or social media. Regarding social media, AI can analyse user content with information about any anomalies and their locations (Kejriwal 2019). These may include, for example, information about unusual weather phenomena or any non-standard animal behaviours.

Social media is additionally an important communication channel during various stages of emergencies or crises, allowing fast and effective communication. For the tool to be used effectively, however, it is necessary to counteract disinformation. It is particularly important in times when information is spreading fast and is not always reliable (Brando 2020). In such an event, AI may be applied in the analysis and management of data streams. This gives rise to another dilemma related to how a given algorithm is to make a distinction between accurate information and disinformation.

Once a natural disaster occurs, AI helps analyse and evaluate damage. It may quickly analyse satellite images and data from UAVs. This, in turn, facilitates the planning of rescue operations and the dispatching of aid to places where it is most needed. Regarding coordinating rescue actions, AI can optimise logistics and the distribution of aid (Khalil et al., 2008). It analyses the needs of the victims and available resources, which allows a more effective division of humanitarian aid. Moreover, in search and rescue operations, AI-controlled robots and drones can search areas affected by a natural disaster, detect victims and deliver required aid. The technology might greatly contribute to increasing the effectiveness and speed of responding to natural disasters. This can save lives and minimise the impact of such events. At the same time, it should be asserted that public administration authorities are

responsible for the planning and preparation of AI resources used in emergencies (Karpiuk 2021, p. 46).

4. The role of artificial intelligence in combating disinformation in the context of crisis management

Universal access to information results in the fact that contemporary societies are struggling with information overload. This makes it difficult to distinguish between reliable and true information and false and manipulated information (Lombardi 2020, p. 13-14). In the face of growing information overload, characterised by the excess and diversity of contents, disinformation has become an effective method for exerting influence.

Disinformation means false information deliberately and often covertly spread to influence public opinion or obscure the truth (Merriam-Webster 2019). In broader terms, it refers to information that is not wholly true or accurate (Learners Dictionary 2019). Disinformation that was historically developing in Russian politics is classified as an action aimed at supporting foreign policy and, as such, it should be separated from intelligence and counter-intelligence, and from traditional diplomacy and informational measures (Active Measures 1986). It should be noted here that the essence of disinformation is the intentional creation and distribution of false or manipulated content to evoke specified social behaviour (Chałubińska-Jentkiewicz, Soler, Makuch 2021). Thus, it might have a destructive impact on the functioning of the state (Chałubińska-Jentkiewicz 2021, p. 14). Disinformation campaigns can indicate that a traditional military operation, or even war, is being prepared. They can also form part of irregular measures combining conventional armed operations with operations carried out by civilians. They are usually long-term campaigns aimed at evoking and amplifying social divides and undermining trust in state institutions (Pietras 2021, p. 25). Disinformation may not only create emergencies but may also be used to escalate social unrest during existing crises (Kaczmarek, 2023, p. 20). Given that, it appears that combating disinformation should be one of the priorities of actions undertaken by entities responsible for crisis management. In the meantime, even democratic states that are strong in economic and military terms do not have effective tools to combat disinformation, and their preventive measures only consist of informational and educational campaigns (Wasilewski 2021, p. 9), which are considered to be critical in counteracting disinformation (Soler, Busiło 2019).

The most straightforward example of evoking or aggravating a crisis because of disinformation measures is a situation where a given population needs to be evacuated. For such evacuation to take place, it is necessary to in-

form the residents of the area concerned. In the meantime, statements negating the need for evacuation or suggesting that the evacuation notice is disinformation might appear in the information space, particularly in social media and online news platforms. Unfortunately, as already mentioned, tools that can effectively counteract such measures are either unavailable or unused. In exceptional circumstances, there should be a possibility for AI to filter information available in a given area according to pre-defined criteria. At the same time, based on the results of analyses, AI algorithms could adjust methods for communicating about existing threats to specified recipients. This might give rise to certain doubts about the ethical aspect of such measures, as citizens are deprived of access to information. However, we should bear in mind that human health and lives should be the highest priority, as evacuation can be ordered as a result of such factors as chemical or radioactive contamination, flood threat or information on a possible terrorist attack. For that reason, if attempts to destabilise social order through disinformation campaigns are detected in cyberspace during an emergency, it is advisable to announce one of the states of exception (Czuryk 2021, p. 86).

Another example where AI could block access to unverified sources of information is a situation where a terrorist attack is being planned to kill as many people as possible. Such an attack could be preceded by a mass disinformation campaign about other events that require the engagement of services. Such actions may be detected and neutralised by AI at the outset. Such planned terrorist attacks might also be preceded by the perpetrators' using the Internet to disseminate information that, on a transport route near the planned attack, there has been a road accident as a result of which cash or other valuable items have been scattered around a vehicle. The publication of such a message could result in jamming all access roads and significantly hindering the work of services that should reach the attack site. Social tensions and emergencies can also be triggered by false information about financial markets or attacks targeting bank infrastructure (Pelc 2020, p. 96). To counteract such situations, AI should also be able to block contents that might evoke adverse social behaviours. In the event of false reports on accidents, catastrophes, etc., AI can analyse information from the Internet of Things (IoT) in real time (Pietryka 2021, p. 25).

5. The prospects of applying the development of artificial intelligence in predicting, managing and preventing emergencies: from distributed systems to image analysis

Predictions concerning the future directions of AI development suggest that we will witness the growth of distributed AI systems, acting independent-

ly in various spheres, and integrated systems that will synchronise data with learning between individual modules. Such an approach will make it possible to create more holistic and effective solutions. AI systems will probably utilise autonomous action in combination with cooperation capabilities, exchange information and learn from other systems. This is likely to contribute to the development of more advanced applications. The analysis of data generated by IoT will play a key role here, allowing real-time monitoring, prediction and response to emergencies. AI will also find its application in the prediction of natural disasters thanks to the possibility to process data from satellites, on-ground sensors and climate models, which will facilitate better forecasting of, for instance, extreme weather conditions whose number has been increasing significantly in recent years (Perdikou et al., 2014, p. 569). The development of AI is also likely to improve the modelling of potential natural disasters by analysing patterns, trends and interdependencies based on historical and current data. Moreover, AI can play a vital part in preventing emergencies, providing a possibility to prepare for such events beforehand based on the results of analyses conducted by such systems. The possibility of early detection of, and fast response to, threats thanks to AI might significantly reduce the risk and effects of crises, including natural and artificial disasters.

In the future, advanced mathematical models used by AI may be crucial for predicting human behaviour that might result in emergencies. The use of AI to analyse CCTV camera images, coupled with deep learning and statistical modelling, is likely to allow the identification of behaviour and action patterns that often precede the occurrence of an emergency. They include aggression, unusual gatherings or non-typical traffic in critical locations.

The AI analysis of camera images might provide information about crowd movement and congestion, behaviours indicating potential violence, or even identify suspicious packages or vehicles. These systems can be programmed to detect specific gestures, facial expressions or other subtle hints that the human eye could miss. Thanks to analysing various data sources, AI can also combine information from cameras with data from other sources, such as social media, telecommunications or meteorological data, to provide the full picture of potential threats.

6. Conclusions

To conclude, the role of AI in crisis management is, without doubt, significant. Thanks to its ability to quickly process and analyse large data sets, AI might contribute to better prediction, monitoring and response to emergencies. This is crucial in preventing natural disasters, handling the consequences of emergencies and combating disinformation that might result in escalating

conflicts or misunderstandings. Nonetheless, emphasis should be placed on the importance of human supervision over AI activities. As has been shown, artificial intelligence algorithms are not free of errors. They could be limited in their actions due to unconscious bias on the part of programmers or limitations of data on which the systems are being trained. Incorrect operation of AI algorithms may also result from learning on outdated and/or erroneous data sets (Surma 2023, p. 40-41). Therefore, it is necessary to continuously monitor and update AI systems to ensure their effectiveness and avoid unintentional consequences.

Furthermore, attention should be paid to the ethical and legal aspects of using AI in crisis management. It is vital to develop a clear legal framework governing the use of AI to protect human rights and ensure accountability for decisions made by algorithms. It is particularly important because such decisions will likely have serious consequences for individuals, societies and states. At the same time, AI-based systems and the information flow between them should be protected against unauthorised access by persons who may use advanced malware for the purpose (Radoniewicz 2021, p. 55).

In the context of future AI development, we can expect enhanced integration and technological advancement in this sphere. AI should be able to analyse a greater number of data sources. This is likely to contribute to better prediction capabilities and faster response to crises. The development of IoT technology, coupled with advanced AI algorithms, might enable far more effective real-time monitoring and crisis management.

The growing significance of analysing images and data from various sensors, which can potentially provide valuable information on the development and scale of crises, is also worth noting. The integration of data with AI systems will facilitate faster identification of threats and better response planning.

Despite the huge potential and benefits that AI might bring in crisis management, we must not forget about maintaining a balance between technological progress and the protection of privacy and human rights. AI should be introduced to crisis management with ethical and social aspects in mind to ensure that this technology serves common interests and does not infringe on fundamental rights and liberties.

Artificial intelligence has immense potential in the sphere of crisis management. Its ability to process large quantities of data and to provide a fast response might significantly contribute to mitigating the impact of crises. However, the intentional and responsible implementation of the technologies is equally important, and all the ethical, legal and social aspects should be regarded. Only then can we guarantee that the benefits that AI might bring will serve everyone, not just selected groups or interests. The future

of AI-supported crisis management seems to be promising, but it requires caution and continuous reflection on the direction of its development and implementation.

AI currently constitutes one of the most advanced technological tools, offering unmatched capabilities related to data analysis, machine learning and automation. However, despite its advanced nature, AI is still a tool, which means that its effectiveness, ethics and use directions depend directly on users' intent and actions. The final impact and results that AI may provide in various sectors – from medicine, through finance, to crisis management – are, to a large extent, shaped by our decisions concerning its programming, implementation, and monitoring. This reminds us of the fundamental principle that technology, irrespective of its advancement level, reflects the values and goals of those who apply it.

References

Active Measures: A Report on the Substance and Process of Anti-U.S. Disinformation and Propaganda Campaigns, p. 1, July 1986, Washington.

Bencsik A., Karpiuk M. (2023). Cybersecurity in Hungary and Poland. Military aspects, *Cybersecurity and Law*, 1, pp. 82-94.

Brando M. (2020). Covid-19 - Comunicazione in emergenza: si insegna nelle università, però nessuno la mette in pratica, https://www.academia.edu/attachments/62873002/download_file?st=MTcwNjU1NTczNiw4My4yMy4xNDYuMTgsMTAwMzQ4MjI%3D&s=profile

Chałubińska-Jentkiewicz K., Soler U., Makuch A. (2023). Disinformation in Polish society in 2021 – trends, channels, sources, *Polish Political Science Yearbook*, 1, pp. 93-107.

Chałubińska-Jentkiewicz, K. (2021) Disinformation – and what else?, *Cybersecurity and Law*, 2, pp. 9-14.

Czuryk M. (2023). Cybersecurity and Protection of Critical Infrastructure, *Studia Iuridica Lublinensia*, 5, pp. 43-52.

Czuryk, M. (2021). Cybersecurity as a premise to introduce a state of exception, *Cybersecurity and Law*, 2, pp. 83-90.

Kaczmarek, K. (2023) Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych, *Roczniki Nauk Społecznych*, 2, pp. 19-30.

Kaczmarek, K. (2023) Zatopione w Morzu Bałtyckim bojowe środki trujące – analiza możliwości wykorzystania ich przez Federację Rosyjską w działaniach terrorystycznych, *Acta Politica Polonica*, 2, pp. 75-82.

Karpiuk M. (2022). Crisis management vs. cyber threats, *Sicurezza, Terrorismo e Societa*, 2, pp. 113-123.

Karpiuk, M. (2021). Cybersecurity as an element in the planning activities of public administration, *Cybersecurity and Law*, 1, pp. 45-52.

Kejriwal M. (2019). Crisis management: Using Artificial Intelligence to help save lives. *Research Outreach*. https://researchoutreach.org/articles/crisis-management-artificial-intelligence-save-lives/

Khalil, K.M., Abdel-Aziz, M., Nazmy, T.T., Salem, A.B.M. (2008). The Role of Artificial Intelligence Technologies in Crisis Response. https://doi.org/10.48550/arXiv.0806.1280

Kostrubiec J. (2021). *Sztuczna inteligencja a prawa i wolności człowieka*, Warsaw.

Kostrubiec, J. (2022). The position of the Computer Security Incidents Response Teams in the national cybersecurity system, *Cybersecurity and Law*, 2, pp. 27-35.

Learnersdictionary (2019). Misinformation, http://www.learnersdictionary.com

Lombardi M. (2020). Communication Crisis: COVID-19. Nothing since Chernobyl. *Sicurezza, Terrorismo e Società*, 12, pp. 7-30.

Merriam-Webster (2019). Disinformation, https://www.merriam-webster.com/

Pelc, P. (2020). The COVID-19 pandemic and the functioning of financial institutions in Poland. Cybersecurity issues, *Cybersecurity and Law*, 1, pp. 93-101.

Perdikou, S., Horak, J., Palliyaguru, R., Halounová, L., Lees, A., Ranguelov, B., & Lombardi, M. (2014). The current landscape of disaster resilience education in Europe. *Procedia Economics and Finance*, 18, pp. 568-575.

Pietras, M. (2021) Wojna informacyjna jako współczesne narzędzie działań nieregularnych, *Cybersecurity and Law*, 2, pp. 21-41.

Pietryka, K. (2021). *Nowe technologie informacyjno-komunikacyjne w zarządzaniu kryzysowym*. In: Danielewska., A., Maciąg, K. (eds.), Wybrane aspekty kryminologii, kryminalistyki i bezpieczeństwa w wymiarze narodowym i międzynarodowym, Lublin, pp. 19-31.

Radoniewicz, F. (2021). Network eavesdropping, *Cybersecurity and Law*, 1, pp. 53-63.

Soler U., Busiło M. (2019). Education of society as a tool to counteract disinformation in implementing new technologies. On the example of 5G mobile telecommunications network and Warsaw sewage system, *Applications of Electromagnetics in Modern Engineering and Medicine (PTZE)* 2019, pp. 210-214.

Surma, J. (2023). *Wprowadzenie do ataków na systemy uczenia maszynowego*. In: Cyberbezpieczeństwo w AI. AI w cyberbezpieczeństwie, Warsaw, pp. 34-44.

Walas-Trębacz, J., Ziarko, J. (2011) *Podstawy zarządzania kryzysowego. Część 2. Zarządzanie kryzysowe w przedsiębiorstwie*, Kraków.

Wasilewski, K. (2021) Fake News and the Europeanization of Cyberspace, *Polish Political Science Yearbook*, 4, issue 50, pp. 61-80.

La Rivista semestrale *Sicurezza, Terrorismo e Società* intende la *Sicurezza* come una condizione che risulta dallo stabilizzarsi e dal mantenersi di misure proattive capaci di promuovere il benessere e la qualità della vita dei cittadini e la vitalità democratica delle istituzioni; affronta il fenomeno del *Terrorismo* come un processo complesso, di lungo periodo, che affonda le sue radici nelle dimensioni culturale, religiosa, politica ed economica che caratterizzano i sistemi sociali; propone alla *Società* – quella degli studiosi e degli operatori e quella ampia di cittadini e istituzioni – strumenti di comprensione, analisi e scenari di tali fenomeni e indirizzi di gestione delle crisi.

Sicurezza, Terrorismo e Società si avvale dei contributi di studiosi, policy maker, analisti, operatori della sicurezza e dei media interessati all'ambito della sicurezza, del terrorismo e del crisis management. Essa si rivolge a tutti coloro che operano in tali settori, volendo rappresentare un momento di confronto partecipativo e aperto al dibattito.

La rivista ospita contributi in più lingue, preferendo l'italiano e l'inglese, per ciascuno dei quali è pubblicato un Executive Summary in entrambe le lingue. La redazione sollecita particolarmente contributi interdisciplinari, commenti, analisi e ricerche attenti alle principali tendenze provenienti dal mondo delle pratiche.

Sicurezza, Terrorismo e Società è un semestrale che pubblica 2 numeri all'anno. Oltre ai due numeri programmati possono essere previsti e pubblicati numeri speciali.

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaterrorismosocieta.it
ISBN: 979-12-5535-352-2