Ius et Securitas 2/2025 | ISSN 3071-799X

Pierre-Alexandre Boudy
Ministry of the Armed Forces (France)
ORCID: 0009-0000-0953-4621
pierrealexandre.boudy@gmail.com

Małgorzata Czuryk
University of Warmia and Mazury in Olsztyn
ORCID: 0000-0003-0362-3791
e-mail: malgorzata.czuryk@uwm.edu.pl

Claudio Melchior
University of Udine
ORCID: 0000-0002-6124-4717
e-mail: claudio.melchior@uniud.it

The Use of New Technologies in the Field of Security

Abstract

The use of new technologies is common, they are used in many areas of human activity, on the one hand, facilitating and streamlining the actions taken in these areas; on the other hand they carry threats that can have far-reaching effects. New technologies are also used in the sphere of security; it is even difficult today to imagine proper protection against threats without new technologies, especially against those that occur in cyberspace.

Artificial intelligence is particularly useful in the security field. It is not yet fully utilized; however, the tendency related to the development and application of artificial intelligence in the security environment is clearly visible in security policy. The use of new technologies in security formations indicates their modernity and greater possibilities for predicting threats, preventing them, responding to them and eliminating their effects.

One of the threats that AI can help combat is disinformation, but AI systems should be used responsibly so as not to increase such threats. AI can be used both to conduct disinformation activities and to counteract them, which is why appropriate protective mechanisms should be introduced at the stage of its programming.

The purpose of the article is to point to new technologies as a potential enabling more effective combating of threats, including those occurring in cyberspace. The article does not discuss the entire spectrum of use of new technologies in the sphere of security, but rather generally refers to their advantages and disadvantages, which concern both the prevention of threats and their generation. The article uses the dogmatic legal method as well as analysis and synthesis.

Keywords: security, new technologies, artificial intelligence, disinformation.

Introduction

New technologies are entering many areas of private life, business, and public activity, and in many of them they are already an inseparable element. The security sphere is no exception because thanks to modern technological solutions, protection against threats becomes more effective. Artificial intelligence takes on particular importance here, which, however, can have a dual application, on the one hand, it can be a tool to combat threats, but on the other it can generate them.

The digital transformation currently underway requires the involvement of many entities in this process, both from the public and private spheres, including the implementation of appropriate policies by the state responsible for its course. It should also be noted that the processes that take place during the digital transformation are determined by international conditions, so it is impossible to introduce appropriate changes in this area in isolation from international policy or international legal solutions. New technologies are not the domain of just one country or several countries, their dimension is global. They affect both the global economy and the public sector, which must also take into account international conditions[1].

In the case of new technologies, special attention should be paid to artificial intelligence, which can significantly contribute to ensuring an appropriate level of security. It should be emphasised that already at the stage of creating artificial intelligence systems capable of analysing data, making decisions, or learning independently, appropriate safeguards must be introduced to protect against their misuse.

It is stressed that the European Union must mobilise its overall innovation capacity and direct significant investments, not only to regain its lead

[1] C. Gaie, M. Karpiuk, A. Spaziani, *New Technologies in Public Administration*, „Ius et Securitas" 2024, No. 1, p. 50.

in new technologies but also to avoid greater technological dependence and to benefit from spillovers in other sectors of the economy. Europe is already witnessing new technological innovations in the security field (including the military). To accelerate the emergence of European technological actors in this area, the regulatory environment must be more risk-friendly[2].

New technologies and security

New technologies are not indifferent to the security environment. They have a real impact on their formation. Without technological development, it is increasingly difficult to counteract threats, which is why investments in this area are necessary. The state must focus on new technologies in its security policy, allowing for more effective protection against threats that threaten security, which is defined as a software or hardware component that supports machine learning, computer vision, natural language understanding, generation, and processing, is becoming increasingly important for ensuring security and also includes robotics. Artificial intelligence enables machines to collect and analyse information about their environment and act towards achieving a given goal[3]. An artificial intelligence system is a machine system that is designed to operate with varying degrees of autonomy and that may exhibit adaptive capabilities after deployment and that, in order to achieve explicit or implicit goals, infers from the input it receives how to generate outputs, such as predictions, content, recommendations, or decisions that may affect physical or virtual environments[4]. In order to achieve the intended objectives of adequate protection against threats, it is important to be able to use artificial intelligence, which, according to Art. 3.56 of the AI Act means the skills, knowledge and understanding that enable providers, implementers, and affected persons (tak-

---

[2] *White Paper for European Defence – Readiness 2030*, Brussels 2025, p. 15.

[3] K. Kaczmarek, *Sztuczna Inteligencja*, [in:] *Leksykon cyberbezpieczeństwa*, K. Chałubińska-Jentkiewicz [ed.], Warszawa 2024, p. 251-252. W sprawie sztucznej inteligencji zobacz także: T. Gergelewicz, *Bipolarity of Artificial Intelligence – Chances and Threats*, „Ius et Securitas" 2024, No. 2, pp. 71-94.

[4] Article 3(1) of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (OJ L 2024/1689), hereinafter referred to as the Artificial Intelligence Act.

ing into account their rights and obligations) to implement AI systems with due awareness, and to be aware of the opportunities and risks associated with AI and the possible harm it may cause.

Artificial intelligence is a technology that more and more armies are investing in because the advantage in the technological race means an advantage on the battlefield. It is being implemented in the armed forces of many countries, and its use supports the army's operations on many levels. Artificial intelligence can be used in building operational awareness, logistics and combat operations[5].

The potential of certain technologies for defensive superiority is an important area that needs to be strengthened at the European level. New technologies are fundamentally changing the nature of warfare in several areas. Artificial intelligence, quantum and cloud computing, advanced and secure communications, autonomous systems, and alternative energy sources have the potential to disrupt and transform traditional approaches to warfare. Drone innovations are already dictating how warfare is fought, the role of robotics is growing, and autonomous ground vehicles are operating in early combat operations. Machines capable of reconnaissance, direct strikes, or logistical support are already influencing the course of battles. However, military robots powered by AI are still in their early stages of development, and Europe has a good chance of achieving greater efficiency in these weapons and the software required to operate them. However, opportunities are shrinking as strategic competitors and rivals invest heavily in these areas, as well as in new technologically complex areas such as hypersonic missiles, guided energy weapons, seabed warfare, and space warfare[6].

It should be emphasised that with a high degree of digitalisation of command processes and autonomy of combat systems, an open armed conflict could quickly occur, therefore decisions regarding the use of armed forces and their individual weapon systems must always be made by humans[7]. Artificial intelligence cannot therefore make decisions in this matter, it should be of a supporting nature, providing information about the threat determining such drastic actions as the use of armed forces.

---

[5] T. Gergelewicz, *Wykorzystanie potencjału sztucznej inteligencji w siłach zbrojnych – wywiad z Chatem GPT*, „Myśl Strategiczna" 2025, No. 2, pp. 10-11.

[6] *White*..., p. 14.

[7] M. Banasik, *Znaczenie nowoczesnych technologii dla bezpieczeństwa*, „Rocznik Bezpieczeństwa Narodowego" 2018, No. 2, p. 129.

In the case of new technologies, cyberspace is used. The Polish Armed Forces include the Cyberspace Defence Forces, which indicates that cyberspace is a very important element of state policy and is also in the sphere of interest of the army, especially considering the fact that cyberattacks can undermine the stability of the state and thus its security (including military security)[8].

Biometrics should also be mentioned, which significantly facilitates ensuring security in the modern world. The use of technologies that identify a given person through unique features for each person, such as fingerprints or iris patterns, eliminates the need to remember complicated passwords and at the same time increases the level of security[9].

Unmanned aerial vehicles are changing the face of modern operational activities. Police and border guards are increasingly using them to patrol border areas and monitor crisis situations. Drones can be equipped with thermal imaging cameras and facial recognition systems, which makes it easier to identify suspects. However, this technology is also used in criminal activities. Organised smuggling groups use drones to transport drugs and weapons, and cybercriminals can use them to carry out attacks on critical infrastructure, disrupting the operation of airports or power grids, among other things. Another technology that can have a significant impact on security is quantum computers. Their high computing power makes it possible to break current encryption standards, which could threaten the security of financial, government, or military data[10].

New technologies play a very important role in the area of security, providing tools that will effectively protect against threats, including those related to unauthorised access to data. In this case, data encryption and blockchain will be of great importance.

Data encryption is a form of cryptography that encodes data in such a way that it becomes unreadable. Text information written in a human-readable language is converted to an encoded language, resulting in unreadable

---

[8] A. Bencsik, M. Karpiuk, M. Kelemen, *The Status of the Armed Forces in Hungary, Poland and Slovakia*, „Ius et Securitas" 2024, No. 1, p. 14.

[9] L. Barcikowski, *Nowoczesne technologie w służbie bezpieczeństwa*, https://www.owobio.edu.pl/nowoczesne-technologie-w-sluzbie-bezpieczenstwa/, [accessed: 15.06.2025].

[10] M. Szpyrka, *Nowe technologie a bezpieczeństwo wewnętrzne UE. Przyszłość w cieniu innowacji*, https://www.euractiv.pl/section/nowe-technologie/news/nowe-technologie-a-bezpieczenstwo-wewnetrzne-ue-przyszlosc-w-cieniu-innowacji/, [accessed: 15.06.2025].

(encrypted) text. Data encryption is a set of techniques to encode sensitive or personal information to ensure its confidentiality. Encryption prevents unauthorised access to data. It remains unreadable to those who do not possess the decryption key[11]. In turn, a blockchain is defined as a record of decentralised data that is securely shared. Blockchain technology allows a group of selected participants to share data. With cloud blockchain services, transaction data from multiple sources can be easily collected, integrated, and shared. Data are divided into shared blocks, linked to unique identifiers in the form of cryptographic hashes[12].

It should be noted that the scientific and technical potential plays a very important role in the area of security. It is indicated that there is a need to provide conditions conducive to the development of innovation, including through state aid in financing projects, their commercialisation and internationalization, as well as counteracting the outflow of human capital. It is also important to promote the development and implementation of new technologies and use their effects for the benefit of security. In order to increase its level, it is necessary to increase expenditure on research and development and increase the efficiency of using the results of these works and their commercialization[13].

New technologies and disinformation as a security threat

Disinformation can also affect the security of a state and pose a major threat to it. It can affect the state's defence and security policy, including its strategic goals related to ensuring independence. Disinformation can interfere with democratic mechanisms, which in turn can result in undermining the stability of the state and also lead to disruptions in the functioning of public authorities. This is also an undesirable phenomenon from the point of view of public interest[14].

[11] *Co to jest szyfrowanie danych?*, https://www.ovhcloud.com/pl/learn/what-is-encryption/, [accessed: 17.06.2025].

[12] *Czym jest blockchain?*, https://www.oracle.com/pl/blockchain/what-is-blockchain/, [accessed: 17.06.2025].

[13] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2020, p. 36

[14] K. Kaczmarek, M. Karpiuk, C. Melchior, *Disinformation as a Threat to State Security*, „Defence Science Review" 2024, No. 20, p. 47.

Artificial intelligence can be used to combat disinformation. AI offers powerful instruments to counter misinformation, although with inherent limitations. Sophisticated machine learning algorithms are capable of discerning characteristic patterns of misinformation through the analysis of text, images, and network data. M. Chora et al. emphasized how machine learning technologies can identify fake news with increasing precision, employing natural language processing (NLP) techniques and tools grounded in reputation and image manipulation[15]. Another example is Botometer, as described by K.C. Yang et al., which analyses social media accounts to detect automated bots spreading misinformation, thus contributing to greater online transparency[16]. J. Pastor-Galindo et al. developed an educational framework based on advanced artificial intelligence models that can simulate disinformation attacks and test defence strategies, thus promoting greater public awareness[17]. These technological developments represent a significant step forward, but raise ethical and operational issues. The automation of detection presents risks of algorithmic bias, lack of transparency, and dependence on limited datasets, which may undermine public trust in such systems. Furthermore, the regulation and application of detection technologies may raise questions about freedom of expression, especially in contexts where technology platforms are used to moderate content.

It is also necessary to keep in mind that artificial intelligence may contribute to disinformation, it remains uncertain which aspect will ultimately prevail, whether the offensive use of AI to generate disinformation or its defensive use to counter it. The rapid advancements in generative models have the potential to render false content increasingly realistic, potentially overwhelming current detection tools. However, the combined progress of 1) advanced algorithm development and 2) public education offers a glimmer of hope. T. Tran et al. emphasises the necessity for reliable tools, observing that many researchers

[15] M. Choraś, K. Demestichas, A. Giełczyk, Á. Herrero, P. Ksieniewicz, K. Remoundou, M. Woźniak, *Advanced machine learning techniques for fake news (online disinformation) detection: A systematic mapping study*, „Applied Soft Computing" 2021, No. 101.

[16] K.C. Yang, O. Varol, C.A. Davis, E. Ferrara, A. Flammini, F. Menczer, *Arming the public with artificial intelligence to counter social bots*, „Human Behavior and Emerging Technologies" 2019, No. 1, pp. 48-61.

[17] J. Pastor-Galindo, P. Nespoli, J.A. Ruipérez-Valiente, *Large-Language-Model-Powered Agent-Based Framework for Misinformation and Disinformation Research: Opportunities and Open Challenges*, „IEEE Security & Privacy" 2024, No. 4.

have tried to tackle the situation by creating misinformation detection systems or algorithms[18]. K.C. Yang et al. also point out that bot detection has become an integral part of the social media experience for many users: 1) but at the same time they underscore that the fight against online manipulation must be carried out by our entire society and not just AI researchers[19].

It should be emphasised that one of the threats occurring in cyberspace is disinformation, therefore, it will be important to understand the mechanisms behind the spread of disinformation and develop methods to counteract its occurrence. Thanks to advanced algorithms and machine learning, it is possible not only to identify, but also to analyse patterns of the spread of false information in real time. These tools allow quick intervention and limiting the harmful impact of disinformation on society. In addition, digital education and raising social awareness related to critical thinking and the verification of information are basic tools in the fight against disinformation. Only by combining technological solutions with education and social awareness can this threat be effectively faced[20].

France: artificial intelligence and the automotive sector in the security context

In France, artificial intelligence has become an integral part of industrial policy, particularly in the automotive sector. This is not just about innovation for its own sake, but about strategic positioning – economic, technological, and increasingly, security-related. The rapid growth of generative AI has pushed car manufacturers to rethink how they design, produce, and manage their vehicles. What used to be a mechanical product is now a digital platform – and France has not stayed on the sidelines. The shift toward the software-defined vehicle (SDV) plays a central role in this transformation. The

[18] T. Tran, R. Valecha, P. Rad, H.R. Rao, *An investigation of misinformation harms related to social media during humanitarian crises*, [in:] *Secure Knowledge Management in Artificial Intelligence Era*, Cham 2020, p. 938.

[19] K.C. Yang, O. Varol, C.A. Davis, E. Ferrara, A. Flammini, F. Menczer, *Arming*..., pp. 48-61.

[20] T. Wojciechowski, *Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego*, „Ius et Securitas" 2024, No. 1, p. 87.

idea is simple: move as much of the vehicle's intelligence as possible into software. In practice, this allows cars to be updated remotely, personalised more easily, and integrated with AI-based features like predictive maintenance or virtual testing. For engineers, it's a new way of thinking. For manufacturers, it's a race to keep up[21].

Renault, one of the key players in the French industry, has chosen a relatively lightweight and flexible path. Rather than building huge internal tech departments, it collaborates with smaller technology firms and startups. Luc Julia, the group's chief scientific officer, openly criticises the idea of overbuilding in-house capacity. He argues that real agility lies in working with specialised partners and being open to external innovation. Renault's strategy is often contrasted with Volkswagen's Cariad project, which aimed to internalise software development but ended up facing major coordination problems and financial losses. Still, the challenges are real. Many French manufacturers struggle to implement AI consistently across their operations. There's often a lack of skilled staff and insufficient links between industrial teams and research labs. Even when the ambition is there, the execution proves difficult. A number of experts point to a broader issue: the French AI ecosystem is strong in talent, but that talent frequently goes abroad—especially to the United States, where access to funding and scale is easier. The French government has not remained passive. Through programmes like France 2030 and the National AI Strategy, it supports public-private partnerships, funds innovation, and promotes the development of secure, ethical, and effective AI applications. The automotive sector is one of the main beneficiaries, not only because of its economic weight, but because of its strategic importance in the shift to connected, autonomous systems[22].

With that, however, come security concerns. A connected vehicle can become a vulnerable one. Hacking, system failures, or even misinformation propagated through in-car systems are no longer science fiction. These risks make the role of cybersecurity, data integrity, and AI robustness a matter of

[21] *Dossier IA – Qui gagnera la guerre de l'IA, la nouvelle révolution automobile?*, https://www.vaylon.fr/dossier-ia-qui-gagnera-la-guerre-de-lia-la-nouvelle-revolution-automobile/, [accessed: 27.06.2025].

[22] *Industry 4.0: France Strategically Invests in AI but ROI Remains Marginal*, https://www.actuia.com/en/news/industry-40-france-strategically-invests-in-ai-but-roi-remains-marginal/, [accessed: 25.06.2025].

public interest. In this sense, France's experience underscores a crucial point: AI in mobility is not just about convenience or cost – it's about control, resilience, and trust.

Conclusions

The process of digital transformation is a great challenge for development in the 21st century. Public and commercial services and industry must take into account the need to have a large amount of data in order to enter the era of artificial intelligence. In recent years, data has become one of the most important factors used in various fields. Acquisition, collection, analysis, processing, and conscious use of data and the constant development of artificial intelligence algorithms are becoming a fundamental principle in force in the world, determining the status of data countries in the global supply chain[23].

In the area of new technologies, the distinction between civilian and defence is blurred. Therefore, innovative civilian startups and the relevant research results and introduced innovations can play a very important role in developing cutting-edge solutions that can significantly increase military capabilities and improve operational readiness in the security sphere. Although Europe is technologically advanced, this does not yet translate into the ability to fully exploit the potential of technology to gain a military advantage. Therefore, there is a need (which should not be postponed) for the European Union to mobilise its overall innovation capacity and direct significant investments to regain the advantage in the field of new technologies[24].

When it comes to the use of new technologies in the sphere of security (including military), special attention should be paid to the armed forces as a qualified instrument of state defence, which need such technologies to meet new challenges and threats. Here, artificial intelligence becomes important, which is the technological driving force of our times, but its bipolarity encourages deeper reflection on its further development. The attractiveness of using artificial intelligence is closely related to its ability to adapt and self-learn, analytical capabilities, which allows the creation of advanced and intelligent systems. One of the most important advantages of artificial intel-

[23] *Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020*, Warszawa 2020, p. 8.
[24] *White*..., p. 14.

ligence is the ability to operate on huge amounts of data and take specific actions based on them[25].

It is noted that it is necessary to encourage private investors in defence, which is related to supporting the financing of projects in the field of common defence and innovation in the field of defence, as well as limiting the associated risks[26].

Bibliography

Banasik M., *Znaczenie nowoczesnych technologii dla bezpieczeństwa*, „Rocznik Bezpieczeństwa Narodowego" 2018, No. 2.

Bencsik A., Karpiuk M., Kelemen M., *The Status of the Armed Forces in Hungary, Poland and Slovakia*, „Ius et Securitas" 2024, No. 1.

Choraś M., Demestichas K., Giełczyk A., Herrero A., Ksieniewicz P., Remoundou K., Woźniak M., *Advanced machine learning techniques for fake news (online disinformation) detection: A systematic mapping study*, „Applied Soft Computing" 2021, No. 101.

Gaie C., Karpiuk M., Spaziani A., *New Technologies in Public Administration*, „Ius et Securitas" 2024, No. 1.

Gergelewicz T., *Bipolarity of Artificial Intelligence – Chances and Threats*, „Ius et Securitas" 2024, No. 2.

Gergelewicz T., *Wykorzystanie potencjału sztucznej inteligencji w siłach zbrojnych – wywiad z Chatem GPT*, „Myśl Strategiczna" 2025, No. 2.

Kaczmarek K., Karpiuk M., Melchior C., *Disinformation as a Threat to State Security*, „Defence Science Review" 2024, No. 20.

Kaczmarek K., *Sztuczna Inteligencja*, [in:] *Leksykon cyberbezpieczeństwa*, K. Chałubińska-Jentkiewicz [ed.], Warszawa 2024.

Leyen U., *Wybór Europy. Wytyczne polityczne na następną kadencję komisji europejskiej 2024–2029*, Strasburg 2024.

Pastor-Galindo J., Nespoli P., Ruipérez-Valiente J.A., *Large-Language-Model-Powered Agent-Based Framework for Misinformation and Disinformation Research: Opportunities and Open Challenges*, „IEEE Security & Privacy" 2024, No. 4.

Tran T., Valecha R., Rad P., Rao H.R., *An investigation of misinformation harms related to social media during humanitarian crises*, [in:] *Secure Knowledge Management in Artificial Intelligence Era*, Cham 2020.

Wojciechowski T., *Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego*, „Ius et Securitas" 2024, No. 1

[25] T. Gergelewicz, *Wykorzystanie*..., p. 6.

[26] Ursula von der Leyen, *Wybór Europy. Wytyczne polityczne na następną kadencję komisji europejskiej 2024–2029*, Strasburg 2024, p. 17.

Yang K.C., Varol O., Davis C.A., Ferrara E., Flammini A., Menczer F., *Arming the public with artificial intelligence to counter social bots*, „Human Behavior and Emerging Technologies" 2019, No. 1.

* * *

Wykorzystanie nowych technologii w sferze bezpieczeństwa

Streszczenie

Wykorzystanie nowych technologii ma charakter powszechny, są one wykorzystywane w wielu obszarach aktywności ludzkiej, z jednej strony ułatwiając i usprawniając działanie podejmowanie w tych obszarach, z drugiej jednak niosą za sobą zagrożenia, które mogą mieć daleko idące skutki. Nowe technologie wykorzystywane są także w sferze bezpieczeństwa, nawet trudno sobie dzisiaj wyobrazić właściwą ochronę przed zagrożeniami bez nowych technologii, zwłaszcza przed tymi, które występują w cyberprzestrzeni.

Szczególne zastosowanie w sferze bezpieczeństwa znajduje sztuczna inteligencja. Nie jest ona jeszcze w pełni wykorzystywana, nie mniej jednak w polityce bezpieczeństwa wyraźnie widoczna jest tendencja związana z rozwojem i stosowaniem sztucznej inteligencji w środowisku bezpieczeństwa. Korzystanie z nowych technologii w formacjach bezpieczeństwa świadczy o ich nowoczesności i większych możliwościach dotyczących przewidywania zagrożeń, zapobiegania im, reagowania na nie oraz usuwania ich skutków.

Jednym z zagrożeń, walkę z którym może wspierać sztuczna inteligencja jest dezinformacja, nie mniej jednak systemy sztucznej inteligencji należy wykorzystywać odpowiedzialnie, żeby nie potęgować takich zagrożeń. Sztuczna inteligencji może służyć zarówno do prowadzenia działań dezinformacyjnych, jak i przeciwdziałać im, dlatego już na etapie jej programowania powinny być wprowadzane odpowiednie mechanizmy ochronne.

Celem artykułu jest wskazanie na nowe technologie, jako potencjał umożliwiający skuteczniejszą walkę z zagrożeniami, w tym również tymi, które występują w cyberprzestrzeni. W artykule nie omówiono całego spektrum wykorzystania nowych technologii w sferze bezpieczeństwa, a ogólnie odniesiono się do ich zalet, a także wad, co dotyczy zarówno zapobiegania zagrożeniom, jak i ich generowania. W artykule zastosowano metodę dogmatyczno-prawną, jak i posłużono sią analizą oraz syntezą.

Słowa kluczowe: bezpieczeństwo, nowe technologie, sztuczna inteligencja, dezinformacja.