Articles

Studia Iuridica Lublinensia vol. 35, 1, 2026
DOI: 10.17951/sil.2026.35.1.41-61

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

Metodi Hadji-Janev
Military Academy General Mihailo Apostolski, North Macedonia
ORCID: 0000-0003-0646-2399
metodi.hadzi-janev@ugd.edu.mk

Mirosław Karpiuk
University of Warmia and Mazury in Olsztyn, Poland
ORCID: 0000-0001-7012-8999
miroslaw.karpiuk@uwm.edu.pl

The Military Dimension of Cybersecurity

Militarny wymiar cyberbezpieczeństwa

ABSTRACT

The development of new technologies, including artificial intelligence, and the widespread use of ICT systems by various entities, including those responsible for ensuring military security, require particular attention to cybersecurity issues. Cybersecurity occupies a prominent place in the military sphere, which is reflected, among others, in the establishment of dedicated structures. Defence against threats emerging in cyberspace, constituting an operational domain, is also an issue dealt with by cyber military units. This article aims to analyse the military aspects of cybersecurity. It argues that cybersecurity in the military dimension is very important for defence. This is particularly true in

CORRESPONDENCE ADDRESS: Pierre-Alexandre Boudy, Ministry of the Armed Forces, France; Metodi Hadji-Janev, PhD, Associate Professor, Military Academy General Mihailo Apostolski (Skopje), Vasko Karangeleski bb, 1000, Skopje, North Macedonia; Mirosław Karpiuk, PhD, Prof. Dr. Habil., Full Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Administrative Law and Security Sciences, Dybowskiego 13, 10-723 Olsztyn, Poland.

a modern, digitised state, which must not only incur public expenses to ensure sufficient protection of the ICT systems used in this sphere but also invest in the digital skills and competencies of personnel responsible for operating these systems. Given the need to identify the status of research on the military dimension of cybersecurity, the literature on the subject was analysed. By applying the doctrinal legal research method, the normative aspects of cybersecurity were identified. In addition, both analytical and synthetic methods were applied.

Keywords: cybersecurity; armed forces; new technologies; artificial intelligence

INTRODUCTION

The modern approach to defence involves the use of new technologies in the military sphere, including modern means of combat and command, and advanced communication systems. Cyberspace constitutes a domain in which interference with state sovereignty can occur without the need for direct military confrontation.

The technological advancement of armed forces and the digitisation of the military sphere generate new threats that may significantly undermine the defence systems of states that rely heavily on ICT systems and are therefore vulnerable to cyberattacks. The technological progress of the armed forces depends, to a large extent, on a state's level of economic development and influences its international position based on sufficient military capabilities to counter new threats, including those occurring in cyberspace. The evolving reality, with the need to adapt to new challenges of the digital world, compels states to adopt new instruments and capabilities in the defence sphere. This has been recognised by many states that establish cyber military units as specialised military formations responsible for cybersecurity in the military dimension.

One can observe a growing role of satellite communications (as a rapid and reliable means of communication), which allows faster information flow, proper military reconnaissance, also in terms of enemy forces and positions, and thus precise identification of targets of potential attacks. However, using such communications triggers the danger of interference with satellite systems, which can paralyse communication and provide incorrect information on an enemy's position.

New technologies in the defence sphere involve innovative solutions that may profoundly change the ways of conducting warfare, responding to threats and handling security issues. Mastering even a few technologies of this sort and applying them to military equipment can offer a significant strategic advantage.[1]

[1] P. Sweklej, A. Seń, M. Szlachta, W. Jagiełło, *Nowe i przełomowe technologie w bezpieczeństwie i obronności priorytety wyborów*, "Wiedza Obronna" 2024, vol. 289(4), p. 24.

CYBERSECURITY IN THE MILITARY DIMENSION

In cyberspace, borders are blurring and the possibilities of supervising the actions performed there are limited. Cyberspace is also where criminals or enemy forces are active, which makes it necessary to ensure adequate protection.[2]

Cybersecurity is defined in European Union law as the activities necessary to protect network and information systems, their users, and other persons affected by cyber threats. Cyberthreats mean any potential circumstances, events or actions that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.[3] Ensuring protection from cyberthreats allows the proper functioning of the state on many levels.[4]

Regarding cybersecurity, the entire security environment and the situation in the international arena must also be taken into consideration, in addition to the ICT infrastructure and the level of digital competence.[5] Cybersecurity forms part of, and cannot be considered in isolation from, security defined as a condition in which individuals, communities, organisations and states are adequately protected against threats that may compromise their well-being, integrity or survival. This involves protecting against physical threats and ensuring stable economic, social, political and environmental conditions.[6] In the case of cybersecurity, threats interfere with the functioning of networks and information systems, the objective of the attacker being to disrupt, degrade, or prevent their normal operation. As such systems

[2] C. Gaie, M. Karpiuk, A. Spaziani, *Cybersecurity in France, Poland and Italy*, "Studia Iuridica Lublinensia" 2025, vol. 34(1), p. 74.

[3] Article 2 (1) and (8) of Regulation of the European Parliament and of the Council (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (OJ L 151/15, 7.6.2019). For more on the definition of cybersecurity, see M. Karpiuk, C. Melchior, U. Soler, *Cybersecurity Management in the Public Service Sector*, "Prawo i Więź" 2023, no. 4, p. 9; M. Czuryk, *Cybersecurity and Protection of Critical Infrastructure*, "Studia Iuridica Lublinensia" 2023, vol. 32(5), pp. 44–45; M. Karpiuk, J. Kostrubiec, *Provincial Governor as a Body Responsible for Combating State Security Threats*, "Studia Iuridica Lublinensia" 2024, vol. 33(1), p. 117.

[4] M. Karpiuk, *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, "Studia Iuridica Lublinensia" 2023, vol. 32(2), p. 190.

[5] K. Kaczmarek, M. Karpiuk, C. Melchior, *A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data*, "Prawo i Więź" 2024, no. 3, pp. 105–106.

[6] K. Kaczmarek, *Wpływ zmian klimatycznych na bezpieczeństwo*, "Journal of Modern Science" 2024, vol. 58(4), p. 412. For more on security, see M. Karpiuk, *Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)*, "Studia Iuridica Lublinensia" 2019, vol. 28(1), pp. 185–194; A. Pieczywok, *Cyberprzestrzeń i dydaktyka cyfrowa na rzecz bezpieczeństwa człowieka*, "Cybersecurity and Law" 2024, vol. 12(2), p. 95; J. Kostrubiec, M. Karpiuk, D. Tyrawa, *The Status of Municipal Government in the Sphere of Ecological Security*, "Hungarian Journal of Legal Studies" 2024, vol. 65(2), pp. 164–181; E. Tkaczyk, *Bezpieczeństwo państwa w Konstytucji Rzeczypospolitej Polskiej. Refleksje nad dobrem chronionym*, "Ius et Securitas" 2024, no. 1, pp. 39–51.

are also used in the military sphere, cyberattacks may threaten state defence and hinder the implementation of effective measures to repel an attack. Therefore, the protection of these systems must be taken into account in the state's defence policy.

The development of new technologies (including military) contributes to a growing use of unmanned and autonomous systems, automated and robotic weapon platforms based on artificial intelligence, as well as long-range precision-guided weapon systems, including ballistic and cruise missiles. The rapid pace of digital transformation requires the effective adoption and management of advanced technological solutions. The development of solutions based on fixed and mobile broadband networks, cloud computing, quantum technology, service automation, machine learning and artificial intelligence provides new development opportunities and, at the same time, generates previously unknown risks. In the context of the digital revolution, special roles played by cyberspace and information space must be taken into account. Both domains create opportunities for spurring disinformation and tampering with facts, which calls for effective strategic communication activities.[7]

Using new technologies in the military sphere makes it possible to improve combat capabilities and, at the same time, enhance protection and resistance to adverse impacts. It also fosters building automated real-time situational awareness through the early detection, identification and classification of threats in different domains. In addition, such technologies enable access to a wide range of data, information and identified activity patterns of an adversary. As a result, they are expected to contribute to an information and decision-making advantage. Access to large volumes of data and the ability to identify behavioural patterns can also improve the forecasting of future events and emerging threats.[8] New technologies require using ICT systems to operate properly, and these are vulnerable to cyberthreats. Consequently, military forces must rely on adequate protection, which requires not only specialist knowledge but also new solutions to be implemented on an ongoing basis (or the existing ones to be properly modified). This, in turn, entails considerable financial outlays. However, it is worth stressing that saving

[7] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2020, pp. 7–8. For more on disinformation, see K. Kaczmarek, *Konsekwencje dezinformacji. Przegląd wybranych narzędzi i technik manipulacji*, "Bezpieczeństwo Narodowe" 2024, vol. 45; M. Ciesielski, *Disinformation in Cyberspace: Introduction to Discussion on Criminalisation Possibilities*, "Cybersecurity and Law" 2024, vol. 11(1); J. Olędzka, *Zjawisko dezinformacji jako źródło zagrożeń bezpieczeństwa państwa – zarys problematyki*, [in:] *Współczesne zagrożenia bezpieczeństwa*, ed. A. Jelonek, Warszawa 2024; P. Pelc, *Cyberprzestrzeń jako element walki informacyjnej – doświadczenia z konfliktu w Ukrainie*, "Bezpieczeństwo Narodowe" 2024, vol. 45(2); T. Gergelewicz, *Informacja sygnalna. Katalog obszarów działań antydezinformacyjnych*, Warszawa 2023; K. Kaczmarek, *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, "Rocznik Nauk Społecznych" 2023, vol. 51(2).

[8] M.M. Fryc, *Nowoczesne technologie kształtujące rozwój sił zbrojnych i ich operacyjne użycie do 2039 roku*, "Bezpieczeństwo Narodowe" 2023, vol. 42(1), pp. 169–170.

too much on defence can bring disastrous consequences. Investment in defence, including modern tools to support both offensive and defensive operations, must keep pace with the changing digital reality requiring the constant monitoring of threats emerging in cyberspace.

Disruptions occurring in cyberspace can adversely influence the functioning of the state and its strategic sectors. Given the need to adequately secure them, it is necessary to take appropriate measures to protect them from cyberthreats.[9] One such strategic sector is the arms sector. It requires significant financial outlay and investment in new technologies. Without such outlay and investment, it will not be competitive or able to supply the army with modern weapons, and without these, any armed conflict in modern times might hardly be won.

A modern army should use artificial intelligence for both defensive and offensive operations. Achievements related to artificial intelligence can be seen in every field.[10] It should be used, to a greater extent, in combating threats (while it should not generate threats itself). Artificial intelligence algorithms can support predicting threats and eliminating them before any adverse effects occur. It can prove useful in both mitigating the consequences and preventing their occurrence in the future. The functioning of artificial intelligence can hardly be analysed without taking into account cybersecurity. The use of advanced digital technologies coupled with artificial intelligence tools must, at any rate, be safe.[11] Artificial intelligence systems can facilitate identifying and combating cyberattacks, thus contributing to increased security in cyberspace. If used properly, artificial intelligence, as a future technology, can serve the purpose of anticipating and neutralising cyberthreats despite their diversity and dynamics. Nonetheless, it should be borne in mind that it can also contribute to such threats and should be used responsibly.[12]

---

[9] M. Karpiuk, *Recognizing an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, "Prawo i Więź" 2022, no. 4, pp. 167–168.

[10] S. Wojtczak, P. Księżak, *Prawo autorskie wobec sztucznej inteligencji (próba alternatywnego spojrzenia)*, "Państwo i Prawo" 2021, no. 2, p. 18.

[11] K. Kaczmarek, M. Karpiuk, A. Spaziani, *Use of Artificial Intelligence in Public Sector: Threats and Prospects*, "Studia Iuridica Toruniensia" 2025, vol. 36(1).

[12] C. Gaie, M. Karpiuk, N. Strizzolo, *Cybersecurity of Public Sector Institutions*, "Prawo i Więź" 2024, vol. 53(6), pp. 356–357. Artificial intelligence is an extremely useful tool, offering new opportunities in many fields. However, it should be borne in mind that it is not a universal solution to all problems and can sometimes do more harm than good. See P. Zaborowski, *Sztuczna inteligencja – wątpliwości, pułapki i obawy*, "Cybersecurity and Law" 2025, vol. 13(1), p. 152. For more on artificial intelligence, see T. Gergelewicz, *Bipolarity of Artificial Intelligence – Chances and Threats*, "Ius et Securitas" 2024, no. 2, pp. 71–94; idem, *Sztuczna inteligencja w perspektywie zagrożeń informacyjnych*, "Przegląd Sił Zbrojnych" 2025, no. 1, pp. 143–145; A. Bencsik, *The Opportunities of Digitalisation in Public Administration with a Special Focus on the Use of Artificial Intelligence*, "Studia Iuridica Lublinensia" 2024, vol. 33(2), pp. 14–17.

Attention should be paid to the legal and ethical contexts of artificial intelligence. The international and technical contexts cannot be underestimated either. International legal solutions must take into consideration the global aspect of artificial intelligence and protect the international community from the negative consequences of its misuse. International cooperation in the field of implementing and evaluating artificial intelligence systems, and exchanging related experience, will also be essential. In addition, when using artificial intelligence, it is important to maintain appropriate ethical standards and ensure respect for fundamental rights, civil liberties, and human dignity.[13] Ensuring cybersecurity may, in some cases, require interference with individual freedoms and rights. However, no such restrictions may infringe on human dignity or be disproportionate to the purpose they are expected to serve.[14] Moreover, restrictions on the exercise of human and civil liberties and rights cannot be imposed automatically. However, the nature of the threat must be analysed on a case-by-case basis.[15]

Improving the combat capability of the armed forces is most often conceptualised as the development of modern technologies, tactics, strategies, and structures. However, adaptation is also necessary, which is the result of combat experience. Therefore, the use of modern technologies in the armed forces is never just about defining and implementing technological solutions, but has four dimensions: new technology that can be used in combat, appropriate employment doctrine, reorganisation of structures, and appropriate training. Focusing on one dimension leads to failures in the process of military transformation. Therefore, innovation must be understood holistically, by including doctrinal reflection, army organisation, and training within military structures.[16]

As the character of conflicts evolves and military operations are increasingly conducted in complex physical, human, and temporal environments, the armed forces must continuously monitor developments in civilian technologies. Significant private-sector investments in areas such as virtual reality, geospatial intelligence and satellite imagery, autonomous systems and drones, energy management, or

[13] D. Bierecki, C. Gaie, M. Karpiuk, *Artificial Intelligence in e-Administration*, "Prawo i Więź" 2025, vol. 54(1), pp. 402–403.

[14] M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(3), p. 32. See also R. Kostrubiec, *Dopuszczalne ograniczenia prawa do swobodnego, pokojowego zgromadzania się w systemie praw człowieka*, Zamość 2024, p. 23; M. Czuryk, *Dopuszczalne różnicowanie sytuacji pracowników ze względu na religię, wyznanie lub światopogląd*, "Studia z Prawa Wyznaniowego" 2024, vol. 27, p. 158.

[15] M. Czuryk, *Activities of the Local Government During a State of Natural Disaster*, "Studia Iuridica Lublinensia" 2021, vol. 30(4), p. 121.

[16] O. Schmitt, *Innover dans les armées: les enjeux du changement militaire,* "Revue Défense Nationale " 2018, vol. 810(5), pp. 25–26.

nanotechnology are driving technological advances that are equally relevant to the defence sector.[17]

In France, one of the key drivers of technological progress within the armed forces is the mobilisation of the creativity and expertise of the diverse actors operating in the field of innovation. This approach aims to address a wide range of challenges, including operational, capability-related, technological, organisational, and industrial issues.[18] Consequently, innovation is regarded as a fundamental source of operational advantage and a critical component of military effectiveness.[19]

The areas of technological research of interest to the French Armed Forces include directed energy, hypersonics, energy security, food security and water security, materials and production, transport systems, quantum technologies, autonomous systems and robotics, hardware and chips, positioning, navigation and timing (PNT), space technologies, biotechnology, synthetic biology, artificial intelligence, big data analytics, communication technologies, digital security, information manipulation and perception, and virtual and augmented reality.[20]

The French Armed Forces took a significant step in their digital transformation by implementing GenIAI.intradef in February 2025. Unlike commercial generative artificial intelligence systems such as ChatGPT, OpenAI, Google's Gemini, or Mistral AI's Le Chat, this platform was developed entirely within the French defence services. This strategic choice aims to guarantee full control over military data and avoid any dependence on potentially foreign entities. The new tool, accessible via the military intranet, is intended exclusively for civilian and military defence personnel. It offers the classic functionalities of a conversational assistant, including answering questions, supporting writing tasks, and stimulating reflection, while also offering translation and document-synthesis services tailored to the specific needs of the armed forces. By creating its own generative artificial intelligence tool, the French Army confirms its desire for technological independence in an area that has become crucial for national defence.[21]

---

[17] E. Chiva, *Nouvelles technologies et art de la guerre*, "Questions Internationales" 2018, vol. 91–92(3), pp. 94–95.

[18] Ministère des Armées et des Anciens combattants, *Innovation et technologie*, https://www.defense.gouv.fr/nos-expertises/innovation-technologie (access: 2.4.2025).

[19] J. Bordellès, T. Fried, *L'innovation à l'État-major des Armées,* "Revue Défense Nationale" 2024, vol. 875(10), pp. 18–19.

[20] Document de référence de l'orientation de l'innovation de défense (DrOID), https://ihedn.fr/veille-strategique/document-de-reference-de-lorientation-de-linnovation-de-defense-2023-droid (access: 7.4.2025).

[21] C. Hessoun, *Europe: l'Armée française fait un pas vers son indépendance dans ce domaine*, 13.3.2025, https://lanouvelletribune.info/2025/03/europe-larmee-francaise-fait-un-pas-vers-son-independance-dans-ce-domaine/?utm_source=chatgpt.com#google_vignette (access: 8.4.2025).

GOVERNANCE AS A STRATEGIC CAPABILITY FOR SOUTH-EASTERN EUROPEAN STATES: THE ROLE OF LEGAL AND ETHICAL FRAMEWORKS IN MILITARY CYBER AND AI OPERATIONS

In the rapidly evolving security landscape of the digital era, legal and ethical governance is no longer a support function – it is a strategic capability.[22] For smaller NATO Allies in South Eastern Europe (SEE), including Albania, Bulgaria, Croatia, Greece, Montenegro, and North Macedonia, meaningful contributions to alliance-wide digital transformation may derive not only from advanced technological capabilities, but also from leadership in establishing normative, legal, and ethical standards that guide the responsible use of military artificial intelligence and cyber operations.[23] These states, many of which are navigating the dual challenge of modernization and resilience-building, are well positioned to shape the trajectory of NATO's digital doctrine by anchoring it in democratic values and rule-of-law principles.[24]

Military cyber operations now span a wide spectrum, ranging from the passive defence of networks to offensive capabilities that can disrupt, degrade, or destroy adversary systems.[25] Meanwhile, AI-enabled systems are increasingly integrated into battlefield decision-making, threat detection, command-and-control, intelligence analysis, and autonomous platforms.[26] These technologies significantly enhance military effectiveness, but they also introduce complex ethical dilemmas and legal grey zones, especially in areas such as attribution, proportionality, unintended escalation, and accountability for autonomous systems' actions. As cyber and AI-enabled operations continue to converge, there is a growing need for governance models that ensure operational effectiveness without compromising legality or moral clarity. NATO's ongoing efforts – such as the Responsible Use Principles for Artificial Intelligence in Defence principles and emerging cyber doctrines – are necessary but require further operationalization and national-level ownership, particularly by member states that can bridge policy and practice with context-sensitive approaches.[27]

The contribution of South-Eastern European countries to cyber and AI operations need not focus solely on building technological parity with larger NATO

[22] NATO, *Summary of the NATO Artificial Intelligence Strategy*, 22.10.2021, https://www.nato.int/cps/en/natohq/official_texts_187617.htm (access: 21.4.2025).

[23] European Commission, *EU Cybersecurity Strategy*, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (access: 2.4.2025).

[24] L. Kello, *The Virtual Weapon and International Order*, New Haven 2017.

[25] NATO, *Cyber Defence*, 30.7.2024, https://www.nato.int/cps/en/natohq/topics_78170.htm (access: 2.4.2025).

[26] G. Allen, T. Chan, *Artificial Intelligence and National Security*, Cambridge 2017.

[27] NATO, *Summary…*

members; instead, countries can take the lead in developing clear rules of engagement, ethical review protocols, and legal interoperability frameworks. This is not to argue that they should shift focus from R&D, but to reconsider important aspects where they could also have a greater impact and contribution. This could include deploying legal experts in joint cyber missions, leading NATO tabletop exercises simulating AI-driven conflict scenarios, and establishing national centres of excellence dedicated to AI and cyber law.[28] By positioning governance as a frontline capability, South-Eastern European countries can demonstrate that responsible innovation is a force multiplier, enhancing trust, fostering coalition coherence, and deterring adversaries who exploit ambiguity in the digital battlespace.

SOVEREIGNTY THROUGH NORMS: A STRATEGIC ADVANTAGE

While larger NATO members may lead in developing cutting-edge military technologies, smaller states are well positioned to assert regulatory sovereignty by shaping the ethical and legal contours of these technologies' use. In an era characterised by hybrid threats, automated decision-making, and disinformation, clarity and legitimacy in how force is applied, particularly in cyberspace, are essential for preserving democratic values and public trust.[29] South-Eastern European countries, many of which have navigated post-conflict democratic transitions, understand the strategic value of legitimacy. Their voices are uniquely credible in advocating for frameworks that embed international humanitarian law, accountability mechanisms, and human oversight into NATO's digital posture.[30]

The principle of "sovereignty through norms" allows smaller allies to exercise influence disproportionate to their size by acting as moral and legal standard-bearers within the Alliance. Countries such as North Macedonia, Montenegro, and Albania can promote normative leadership by developing doctrine, hosting multilateral legal working groups, or chairing NATO expert panels on AI governance or cyber accountability. Such engagement not only reinforces NATO cohesion but may also strengthen national sovereignty by ensuring that these states participate in the formulation of strategic digital policies rather than remaining passive recipients of external policy frameworks. Through the exercise of normative agency, South-Eastern European countries can protect their democratic trajectories while actively shaping the rules that will govern future conflicts.

---

[28] European Defence Agency, *The 2023 EU Capability Development Priorities*, https://eda.europa.eu/docs/default-source/brochures/qu-03-23-421-en-n-web.pdf (access: 24.4.2025).

[29] NATO, *Summary…*.

[30] UNIDIR, *The Global Kaleidoscope of Military AI Governance*, 5.9.2024, https://unidir.org/publication/the-global-kaleidoscope-of-military-ai-governance (access: 30.4.2025).

Furthermore, this normative influence provides important strategic value in countering authoritarian models of digital warfare, which often prioritize efficiency and control over legality and ethics. Adversarial actors such as Russia and China continue to advance techno-authoritarian norms, employing cyber and artificial intelligence capabilities to influence, coerce, and destabilize democratic societies.[31] By contrast, the SEE region – given its proximity to active zones of hybrid conflict and its integration into Euro-Atlantic structures – can play a constructive role in reinforcing democratic resilience. The articulation of digital sovereignty rooted in transparency, rule of law, and accountability may serve as a soft power counterweight to authoritarian digital statecraft, reinforcing NATO's value-based identity in the information domain.

Moreover, embracing normative leadership supports domestic resilience. By embedding ethical standards into cyber defence and AI usage, South-Eastern European countries can foster greater inter-agency trust, strengthen judicial engagement, and increase public awareness. This contributes to bridging the civilian–military divide in digital security governance and supports the integration of ethical tech frameworks into national security strategies, procurement policies, and legislative reforms. Initiatives such as citizen-centered digital literacy campaigns, artificial intelligence ethics advisory bodies, and legal audits of offensive cyber operations can all serve to anchor national policy in democratic oversight. In doing so, these states not only enhance their security but also strengthen their credibility as partners in international coalitions.[32]

The strategic advantage of smaller NATO Allies lies not in matching the military-industrial scale of larger nations, but in offering clarity, credibility, and constraint. South-Eastern European countries can play a leading role in defining what responsible cyber and AI operations should look like in democratic societies. By doing so, they reinforce NATO's normative coherence, enhance regional interoperability, and ensure that digital sovereignty is exercised not through domination, but through shared norms. In a future increasingly shaped by autonomous technologies and contested information spaces, those who set the rules will shape the battlefield, and smaller nations that lead with principles will punch well above their weight.

By proactively contributing to the legal and ethical governance of cyber and AI operations, South-Eastern European countries may play a crucial role in the formation of state practice, a foundational element in the development of customary international law – *opinio juris*.[33] Through national legislation, doctrinal publica-

[31] L. Kovachich, A. Kolesnikov, *Digital Authoritarianism with Russian Characteristics?*, 21.4.2021, https://carnegieendowment.org/posts/2021/06/digital-authoritarianism-with-russian-characteristics (access: 30.4.2025).

[32] NATO, *Emerging and Disruptive Technologies*, https://www.nato.int/cps/en/natohq/topics_184303.htm (access: 2.5.2025).

[33] M. Wood, O. Sender, *State Practice*, Oxford 2020.

tions, participation in NATO policy forums, and joint exercises with embedded ethical frameworks, these countries demonstrate consistent, deliberate behavior that reflects a commitment to rule-based digital conduct. Over time, such actions may shape emerging norms, particularly regarding the lawful use of autonomous systems, the attribution and proportionality of cyber responses, and the safeguarding of civilian infrastructure in digital conflict. As South-Eastern European countries institutionalize transparency, human oversight, and compliance with international humanitarian law, they help crystallize a collective Euro-Atlantic vision for responsible state behavior in cyberspace and artificial intelligence governance.

This contribution also strengthens the Euro-Atlantic normative position in a rapidly polarizing global context. As authoritarian regimes such as China and Russia seek to advance techno-sovereignty models that elevate state control and suppress accountability, South-Eastern European countries' leadership in embedding democratic values into emerging digital norms serves as a compelling counter-narrative.[34] By aligning strategic sovereignty with ethical multilateralism, these countries not only insulate their own institutions from foreign manipulation but also reinforce the legitimacy of NATO's value-based approach to the digital domain. Their engagement lends credibility and diversity to the Euro-Atlantic bloc's normative claims, helping to contest authoritarian efforts to dominate global regulatory discourse around cyber and artificial intelligence technologies. In doing so, SEE NATO Allies help ensure that international law evolves in a direction that prioritizes transparency, accountability, and human dignity over coercion and opacity.[35]

HARMONIZING NATIONAL FRAMEWORKS WITH NATO AND EU STANDARDS

A key area of strategic contribution lies in the harmonization of national legislation with NATO doctrines and emerging EU regulations such as the NIS 2 Directive,[36] the AI Act,[37] and the EU Cyber Solidarity Act.[38] This alignment not only facilitates interoperability in joint cyber operations but also strengthens resilience through trusted legal environments. It enables secure intelligence-sharing, supports

[34] D. Flonk, *Emerging Illiberal Norms: Russia and China as Promoters of Internet Sovereignty*, 13.5.2022, https://www.illiberalism.org/danielle-flonk-emerging-illiberal-norms-russia-and-china-as-promoters-of-internet-content-control (access: 2.5.2025).

[35] FIIA, *Digital Authoritarianism in China and Russia: Common Goals and Diverging Standpoints in the Era of Great-Power Rivalry*, https://fiia.fi/en/publication/digital-authoritarianism-in-china-and-russia (access: 2.5.2025).

[36] https://www.nis-2-directive.com (access: 2.5.2025).

[37] https://artificialintelligenceact.eu (access: 4.5.2025).

[38] https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity (access: 4.5.2025).

the lawful use of dual-use technologies, and ensures that ethical considerations are not sidelined in operational planning.[39] These efforts demonstrate how legal infrastructure can evolve alongside technological innovation – rather than lag behind it.

For SEE NATO Allies, this harmonization process represents more than compliance; it is a conscious exercise in asserting legal sovereignty and embedding democratic values into the digital domain. By tailoring national strategies, cybersecurity laws, and artificial intelligence governance mechanisms to reflect both NATO operational needs and EU normative frameworks, these countries ensure their dual integration into Euro-Atlantic security structures.[40] This dual alignment also allows South-Eastern European states to serve as legal and policy bridges between transatlantic and European regulatory regimes, especially vital in the context of joint missions, multinational cyber coalitions, and the defence of shared digital infrastructure.[41]

Moreover, as threats grow more complex – spanning from cyber-enabled espionage to the militarization of misinformation – national frameworks must be agile enough to absorb NATO's threat intelligence protocols and the EU's regulatory innovations in real time. South-Eastern European countries are increasingly investing in adaptive regulatory ecosystems, where threat assessments, data protection standards, and AI transparency requirements can be revised in tandem with geopolitical developments. This capacity for synchronized legal evolution makes them valuable contributors to both strategic foresight and operational readiness within the alliance.

By embedding harmonized legal frameworks into national defence and digital transformation strategies, South-Eastern European countries not only safeguard their own digital sovereignty but also reinforce the cohesion of NATO and the EU.[42] These states showcase how principled legal adaptation can serve as a force multiplier – ensuring that interoperability is not merely technical but also ethical and lawful. In doing so, they help future-proof NATO's digital capabilities against the legal fragmentation and normative ambiguity often exploited by hostile actors. Their leadership in legal harmonization is therefore not peripheral, but central to building a resilient, values-based Euro-Atlantic security architecture in the age of cyber and AI operations.

By harmonizing national frameworks with both NATO doctrines and EU regulatory efforts, South-Eastern European countries are uniquely positioned to help bridge the emerging friction between calls for strong regulation and the need to

[39] NATO, *Cyber Defence…*

[40] *NIS2: Enhancing Cyber Resilience Across the EU*, https://www.enisa.europa.eu (access: 4.5.2025).

[41] NATO, *Emerging…*

[42] *Legal Frameworks in Cyber Defence*, https://ccdcoe.org (access: 4.5.2025).

sustain technological innovation.[43] Under-regulation risks eroding public trust, weakening interoperability, and leaving legal gaps that adversaries can exploit.[44] South-Eastern European nations, through balanced legal transposition and operational alignment, can model how regulation and innovation are not mutually exclusive but mutually reinforcing.

OPERATIONALIZING ETHICS IN DEFENCE INNOVATION

As artificial intelligence becomes increasingly integrated into NATO command-and-control, surveillance, and autonomous systems, South-Eastern European countries can play a leading role in advancing ethics-by-design methodologies. Embedding ethical principles – such as fairness, explainability, and proportionality – during the development phase of military AI systems ensures that human rights and operational effectiveness are not treated as competing interests, but as mutually reinforcing goals. This is especially vital in the context of blurred civil–military boundaries, where public trust in digital transformation of defence depends on robust oversight and transparent legal safeguards.

South-Eastern European countries possess a strategic advantage in this area due to their ongoing institutional modernization and lessons learned from navigating democratic consolidation. Their defence sectors are often transforming, making them more open to integrating human-centred design principles from the ground up rather than retrofitting them later. This "clean slate" opportunity allows SEE Allies to serve as testbeds for operationalizing ethical artificial intelligence through doctrinal updates, procurement frameworks, and collaboration with academia and civil society, providing a tangible model for larger NATO Allies facing more entrenched institutional inertia.

Moreover, these efforts can contribute to NATO's broader ethical framework development by offering tested use cases and scalable models. By actively participating in NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) and engaging with EU innovation initiatives like the European Defence Fund, South-Eastern European countries can help ensure that ethical artificial intelligence is treated not as an abstract principle, but as a practical and mission-relevant standard. Their engagement may also encourage responsible innovation pathways for dual-use technologies, reducing the risk of ethical backsliding under operational pressure.

---

[43] H. Young, *Harmonizing Cybersecurity Regulations Is a Win-Win*, 10.7.2024, https://techpost.bsa.org/2024/07/10/harmonizing-cybersecurity-regulations-is-a-win-win (access: 5.5.2025).

[44] A. Omena, *The Impact of Emerging Technologies on Legal Frameworks: A Model for Adaptive Regulation*, "International Journal of Research Publication and Reviews" 2024, vol. 5(7), pp. 5046–5060.

Operationalising ethics also requires embedding accountability mechanisms into AI-enabled decision-making processes, particularly in contexts involving autonomous targeting or cyber defence escalation. South-Eastern European countries, with their recent legal harmonisation efforts and proximity to both EU and NATO compliance regimes, are well-positioned to develop oversight tools such as algorithmic auditing, ethics review boards, and human-in-the-loop protocols. These instruments help ensure that military innovation aligns with democratic values, even as the speed and complexity of conflict increase.

Finally, promoting ethical military innovation allows South-Eastern European states to project strategic credibility beyond their size or defence budgets.[45] In the geopolitical contest over the norms governing emerging technologies, authoritarian regimes often prioritise efficiency and control over legality and individual rights. By contrast, SEE countries can demonstrate that ethical artificial intelligence and responsible innovation are not only compatible with strategic advantage, but foundational to it. This enhances their diplomatic weight within NATO and the European Union while helping anchor the Euro-Atlantic normative model in an increasingly polarising global tech order.

NORM ENTREPRENEURSHIP AND MULTILATERAL COALITIONS

Smaller NATO Allies have historically played a key role in building coalitions around shared values, and this extends naturally into cyber and artificial intelligence governance. South-Eastern European states can act as norm entrepreneurs within NATO and other multilateral forums, advocating for binding principles on autonomous weapons, escalation control in cyber conflict, and human accountability in AI-enabled decision-making.[46] Their lived experience with hybrid threats – ranging from disinformation campaigns to foreign malign influence – adds valuable insight into the real-world implications of unchecked digital militarization.

This unique positioning allows South-Eastern European countries to champion a preventive and principled approach in shaping global digital security norms. Their advocacy can contribute to closing the current governance gaps that exist in areas such as the use of lethal autonomous weapons, the deployment of artificial intelligence in surveillance, and offensive cyber operations. By articulating these issues through the lens of democratic fragility, societal trust, and the rule of law, South-Eastern European states can galvanise support from like-minded allies, espe-

[45] D. Baumann, *Military Ethics: A Task for Armies*, "Military Medicine" 2007, vol. 172(2), pp. 34–38.

[46] More about this concept and early writings see I. Christine, *Norm Entrepreneurs: Scandinavia's Role in World Politics*, "Cooperation and Conflict" 2002, vol. 37(1), pp. 11–23.

cially in Central and Eastern Europe, and act as a bridge between Western European standards and the concerns of nations more exposed to geopolitical contestation.

South-Eastern European countries can also play a proactive role in institutional innovation within NATO and the European Union by supporting the establishment of norm-setting bodies or working groups specifically focused on emerging technologies. Initiatives such as an EU–NATO Joint Committee on Ethical Artificial Intelligence in Defence, or a Southeastern Europe Coalition on Cyber Norms could serve as platforms for norm diffusion, transparency, and trust-building. These coalitions would provide a structured mechanism for influencing doctrine, standard-setting, and procurement criteria in a way that aligns with democratic governance and operational needs.

Beyond Euro-Atlantic structures, SEE Allies can leverage their partnerships in the United Nations, the Organization for Security and Co-operation in Europe, and regional security forums to advocate for interoperability between national, alliance, and international norms. In doing so, they help prevent fragmentation in international law and guard against the proliferation of authoritarian interpretations of digital sovereignty and warfare. Through diplomatic outreach, capacity-building initiatives, and technical assistance, South-Eastern European countries can extend their normative influence and foster consensus on critical legal principles such as distinction, proportionality, and accountability in digital operations.

Furthermore, acting as norm entrepreneurs enhances the diplomatic relevance of South-Eastern European countries in the current geopolitical environment, where normative leadership is increasingly contested. With authoritarian regimes promoting state-centric, opaque, and militarized approaches to artificial intelligence and cyber governance, there is a pressing need for credible counter-narratives that promote multilateralism, transparency, and rights-based regulation.[47] South-Eastern European states, by drawing on their democratic transitions and security vulnerabilities, are well-suited to articulate a compelling and actionable vision for responsible digital power – one that reinforces the Euro-Atlantic values architecture while addressing the unique challenges of a multipolar technological world.

These efforts in norm entrepreneurship can serve as a force multiplier for South-Eastern European countries' influence in strategic alliances. By aligning their legal, policy, and diplomatic initiatives with emerging multilateral agendas, they position themselves not merely as norm takers but as norm shapers. This enhances their standing within NATO and the European Union, strengthens regional cohesion, and ensures that their experiences and perspectives help steer the evolving rules of engagement for cyber and AI-enabled warfare.

[47] REMIT, *Summary of the first REMIT Conference: New Perspectives for Technology and Multilateralism, Held on May 16–17, 2024 at KU Leuven*, https://www.remit-research.eu/wp-content/uploads/2024/06/REMIT_Leuven_conference_summary_2024.pdf (access: 16.5.2025).

BUILDING CAPACITIES FOR LEGAL AND ETHICAL LEADERSHIP

To institutionalize their emerging leadership in the normative dimensions of digital defence, South-Eastern European countries must invest in structured capacity-building that bridges operational realities with legal and ethical imperatives. This means moving beyond ad hoc policy responses and establishing enduring mechanisms that embed legal foresight, ethical design, and multilateral interoperability into defence innovation. A strategic starting point would be the creation of national or regional centers of excellence dedicated to the legal and ethical governance of defence technologies. These centers could serve as hubs for interdisciplinary research, NATO-aligned training programs, and cross-sectoral engagement, integrating expertise from military law, technology ethics, cybersecurity, and international relations.

Additionally, the deployment of legal advisory teams to NATO-led cyber exercises and joint operations would allow South-Eastern European countries to shape real-time doctrinal evolution while refining their own strategic acumen. Such advisors could assess operational plans for compliance with International Humanitarian Law, advise on proportionality and accountability in the use of AI-enabled systems, and identify areas of legal ambiguity before crises emerge.[48] Their participation would also help ensure that national interpretations of legal obligations are consistently integrated into NATO's collective decision-making frameworks, enhancing both legitimacy and operational coherence.

South-Eastern European countries are also well-positioned to assume leading roles in drafting, piloting, and stress-testing NATO's evolving governance frameworks on topics such as AI assurance, responsible innovation, cyber rules of engagement, and digital escalation control. Their capacity to act as bridge-builders between national legislatures, regional political blocs, and NATO's strategic command structures gives them unique leverage in aligning democratic values with the Alliance's operational needs. This contribution is particularly crucial as NATO scales up its Digital Transformation Implementation Strategy and explores new domains of deterrence in the cyber and cognitive spheres.

Equally important is the cultivation of inclusive democratic oversight through civil–military–legal dialogue. By engaging legal scholars, civil society, and national security institutions in sustained conversation, South-Eastern European countries can foster a normative ecosystem where societal values shape defence policies, not the other way around. Such inclusive governance not only builds public trust in the digital transformation of the defence sector but also inoculates democracies against the risks of militarized AI applications that lack accountability or transparency.

[48] M. Kempton, E. Parmiggiani, P. Vassilakopoulou, *Accountability in Managing Artificial Intelligence: State of the Art and a Way Forward for Information Systems Research*, 2023, https://aisel.aisnet.org/ecis2023_rp/361 (access: 9.5.2025).

Building legal and ethical leadership capacities is not a secondary or supporting function – it is a strategic investment in long-term resilience, alliance credibility, and global normative influence. By institutionalizing this leadership, South-Eastern European countries can play a formative role in shaping the operational, legal, and moral landscape of NATO's digital future.

CONCLUSIONS

Ensuring independence is conditional, first and foremost, on systemic solutions fostering the mobilisation and operational development of the armed forces, their organisational status, the quantity and quality of staff reserves, the ability to use material and engineering equipment, the ability to respond flexibly to any disruptions in the process of attaining higher levels of defence readiness, and financial outlays on defence. The ability to maintain operational continuity contributes to establishing the conditions conducive for the army to accomplish its operational objectives. However, it requires the maintenance of adequate military capabilities and equipment, the timely replenishment of reserves, combat assets and material, both within and beyond the state borders, and the effective recovery of losses and staff rotation. Operational effectiveness enables the efficient use of the state's military potential and means displaying adequate range and accuracy of fire. This objective can be achieved through modern command systems, effective reconnaissance and intelligence, the availability of military forces, planning and command procedures, the optimal use of combat assets, the preservation of stock and combat assets, and military training.[49] Solutions to ensure a high level of operational effectiveness of the armed forces must include (in addition to conventional operations) the capabilities of contemporary warfare in cyberspace. The modern army must use tools to target the enemy's actions accurately and quickly. This purpose is served precisely by ICT systems. New technologies are essential for military forces with a highly developed arms industry. Without such technologies, the state cannot enjoy adequate protection.

Attention should also be paid to artificial intelligence systems in the defence sphere. In the armed forces, it is already an indispensable technology and every modern army must have it at its disposal so as not to be underestimated by its adversaries. In the military sphere, there are numerous areas where artificial intelligence can come in handy. As the international defence environment continues to evolve, investing in the acquisition and deployment of artificial intelligence

[49] L. Elak, K. Walczuk, *Anti-Access/Area-Denial Operation of the Russian Federation in Light of an Article 5 of the Constitution of the Republic of Poland*, "Wiedza Obronna" 2024, vol. 288(3), p. 215.

systems, which influence all domains of operational activities in the armed forces, appears indispensable. The purpose of artificial intelligence in the military forces is to gain an advantage over the adversary in all aspects of military operations – reconnaissance, command, missile, protection or logistical security. Nonetheless, while bringing numerous benefits, artificial intelligence also involves certain risks. Therefore, it must be used in line with its intended purpose and loss of control over its functioning must be avoided.

It has become essential to engage in activities fostering technological development and enabling a tangible impact on such development, rather than merely benefiting from its effects. If the state's role is reduced to merely using new technologies, it will not be on an equal footing with those states that contribute to shaping modern digital tools. This may ultimately weaken its international position (including in the field of defence, where such tools are used).

The ability to ensure that military artificial intelligence and cyber operations remain lawful, accountable, and aligned with democratic values constitutes an important element of contemporary deterrence. For smaller Allies in South Eastern Europe, contributing to NATO's digital transformation does not require matching technological scale – it requires providing governance leadership. By doing so, these states help anchor emerging technologies within a framework of legitimacy and trust, reinforcing both national security and alliance cohesion in the digital age.

REFERENCES

Literature

Allen G., Chan T., *Artificial Intelligence and National Security*, Cambridge 2017.

Baumann D., *Military Ethics: A Task for Armies*, "Military Medicine" 2007, vol. 172(2). **DOI: https://doi.org/10.7205/MILMED.173.Supplement_2.34**

Bencsik A., *The Opportunities of Digitalisation in Public Administration with a Special Focus on the Use of Artificial Intelligence*, "Studia Iuridica Lublinensia" 2024, vol. 33(2). **DOI: https://doi.org/10.17951/sil.2024.33.2.11-23**

Bierecki D., Gaie C., Karpiuk M., *Artificial Intelligence in e-Administration*, "Prawo i Więź" 2025, vol. 54(1). **DOI: https://doi.org/10.36128/PRIW.VI54.1201**

Bordellès J., Fried T., *L'innovation à l'État-major des Armées,* "Revue Défense Nationale" 2024, vol. 875(10). **DOI: https://doi.org/10.3917/rdna.875.0018**

Chiva E., *Nouvelles technologies et art de la guerre*, "Questions Internationales" 2018, vol. 91–92(3). **DOI: https://doi.org/10.3917/quin.091.0094**

Christine I., *Norm Entrepreneurs: Scandinavia's Role in World Politics*, "Cooperation and Conflict" 2002, vol. 37(1).

Ciesielski M., *Disinformation in Cyberspace: Introduction to Discussion on Criminalisation Possibilities*, "Cybersecurity and Law" 2024, vol. 11(1).

Czuryk M., *Activities of the Local Government During a State of Natural Disaster*, "Studia Iuridica Lublinensia" 2021, vol. 30(4). **DOI: https://doi.org/10.17951/sil.2021.30.4.111-124**

Czuryk M., *Cybersecurity and Protection of Critical Infrastructure*, "Studia Iuridica Lublinensia" 2023, vol. 32(5). **DOI: https://doi.org/10.17951/sil.2023.32.5.43-52**

Czuryk M., *Dopuszczalne różnicowanie sytuacji pracowników ze względu na religię, wyznanie lub światopogląd*, "Studia z Prawa Wyznaniowego" 2024, vol. 27. **DOI: https://doi.org/10.31743/spw.17518**

Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(3). **DOI: https://doi.org/10.17951/sil.2022.31.3.31-43**

Elak L., Walczuk K., *Anti-Access/Area-Denial Operation of the Russian Federation in Light of an Article 5 of the Constitution of the Republic of Poland*, "Wiedza Obronna" 2024, vol. 288(3).

Fryc M.M., *Nowoczesne technologie kształtujące rozwój sił zbrojnych i ich operacyjne użycie do 2039 roku*, "Bezpieczeństwo Narodowe" 2023, vol. 42(1). **DOI: https://doi.org/10.59800/bn/170903**

Gaie C., Karpiuk M., Spaziani A., *Cybersecurity in France, Poland and Italy*, "Studia Iuridica Lublinensia" 2025, vol. 34(1). **DOI: https://doi.org/10.17951/sil.2025.34.1.73-95**

Gaie C., Karpiuk M., Strizzolo M., *Cybersecurity of Public Sector Institutions*, "Prawo i Więź" 2024, vol. 53(6). **DOI: https://doi.org/10.36128/PRIW.VI53.1129**

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

Gergelewicz T., *Informacja sygnalna. Katalog obszarów działań antydezinformacyjnych*, Warszawa 2023.

Gergelewicz T., *Sztuczna inteligencja w perspektywie zagrożeń informacyjnych*, "Przegląd Sił Zbrojnych" 2025, no. 1.

Kaczmarek K., *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, "Rocznik Nauk Społecznych" 2023, vol. 51(2). **DOI: https://doi.org/10.18290/rns2023.0017**

Kaczmarek K., *Konsekwencje dezinformacji. Przegląd wybranych narzędzi i technik manipulacji*, "Bezpieczeństwo Narodowe" 2024, vol. 45. **DOI: https://doi.org/10.59800/bn/196693**

Kaczmarek K., *Wpływ zmian klimatycznych na bezpieczeństwo*, "Journal of Modern Science" 2024, vol. 58(4).

Kaczmarek K., Karpiuk M., Melchior C., *A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data*, "Prawo i Więź" 2024, no. 3. **DOI: https://doi.org/10.36128/PRIW.VI50.907**

Kaczmarek K., Karpiuk M., Spaziani A., *Use of Artificial Intelligence in Public Sector: Threats and Prospects*, "Studia Iuridica Toruniensia" 2025, vol. 36(1). **DOI: https://doi.org/10.12775/SIT.2025.002**

Karpiuk M., *Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)*, "Studia Iuridica Lublinensia" 2019, vol. 28(1). **DOI: https://doi.org/10.17951/sil.2019.28.1.185-194**

Karpiuk M., *Recognizing an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, "Prawo i Więź" 2022, no. 4. **DOI: https://doi.org/10.36128/priw.vi42.524**

Karpiuk M., *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, "Studia Iuridica Lublinensia" 2023, vol. 32(2). **DOI: https://doi.org/10.17951/sil.2023.32.2.189-201**

Karpiuk M., Kostrubiec J., *Provincial Governor as a Body Responsible for Combating State Security Threats*, "Studia Iuridica Lublinensia" 2024, vol. 33(1). **DOI: https://doi.org/10.17951/sil.2024.33.1.107-122**

Karpiuk M., Melchior C., Soler U., *Cybersecurity Management in the Public Service Sector*, "Prawo i Więź" 2023, no. 4. **DOI: https://doi.org/10.36128/PRIW.VI47.751**

Kello L., *The Virtual Weapon and International Order*, New Haven 2017. **DOI: https://doi.org/10.2307/j.ctt1trkjd1**

Kostrubiec J., Karpiuk M., Tyrawa D., *The Status of Municipal Government in the Sphere of Ecological Security*, "Hungarian Journal of Legal Studies" 2024, vol. 65(2). **DOI: https://doi.org/10.1556/2052.2024.00510**

Kostrubiec R., *Dopuszczalne ograniczenia prawa do swobodnego, pokojowego zgromadzania się w systemie praw człowieka*, Zamość 2024.

Olędzka J., *Zjawisko dezinformacji jako źródło zagrożeń bezpieczeństwa państwa – zarys problematyki*, [in:] *Współczesne zagrożenia bezpieczeństwa*, ed. A. Jelonek, Warszawa 2024.

Omena A., *The Impact of Emerging Technologies on Legal Frameworks: A Model for Adaptive Regulation*, "International Journal of Research Publication and Reviews" 2024, vol. 5(7). **DOI: https://doi.org/10.55248/gengpi.5.1024.3012**

Pelc P., *Cyberprzestrzeń jako element walki informacyjnej – doświadczenia z konfliktu w Ukrainie*, "Bezpieczeństwo Narodowe" 2024, vol. 45(2). **DOI: https://doi.org/10.59800/bn/196691**

Pieczywok A., *Cyberprzestrzeń i dydaktyka cyfrowa na rzecz bezpieczeństwa człowieka*, "Cybersecurity and Law" 2024, vol. 12(2).

Schmitt O., *Innover dans les armées: les enjeux du changement militaire,* "Revue Défense Nationale " 2018, vol. 810(5). **DOI: https://doi.org/10.3917/rdna.810.0025**

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020.

Sweklej P., Seń A., Szlachta M., Jagiełło W., *Nowe i przełomowe technologie w bezpieczeństwie i obronności priorytety wyborów*, "Wiedza Obronna" 2024, vol. 289(4).

Tkaczyk E., *Bezpieczeństwo państwa w Konstytucji Rzeczypospolitej Polskiej. Refleksje nad dobrem chronionym*, "Ius et Securitas" 2024, no. 1.

Wojtczak S., Księżak P., *Prawo autorskie wobec sztucznej inteligencji (próba alternatywnego spojrzenia)*, "Państwo i Prawo" 2021, no. 2.

Wood M., Sender O., *State Practice*, Oxford 2020.

Zaborowski P., *Sztuczna inteligencja – wątpliwości, pułapki i obawy*, "Cybersecurity and Law" 2025, vol. 13(1).

Online sources

Document de référence de l'orientation de l'innovation de défense (DrOID), https://ihedn.fr/veille-strategique/document-de-reference-de-lorientation-de-linnovation-de-defense-2023-droid (access: 7.4.2025).

European Commission, *EU Cybersecurity Strategy*, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (access: 2.4.2025).

European Defence Agency, *The 2023 EU Capability Development Priorities*, https://eda.europa.eu/docs/default-source/brochures/qu-03-23-421-en-n-web.pdf (access: 24.4.2025).

FIIA, *Digital Authoritarianism in China and Russia: Common Goals and Diverging Standpoints in the Era of Great-Power Rivalry*, https://fiia.fi/en/publication/digital-authoritarianism-in-china-and-russia (access: 2.5.2025).

Flonk D., *Emerging Illiberal Norms: Russia and China as Promoters of Internet Sovereignty*, 13.5.2022, https://www.illiberalism.org/danielle-flonk-emerging-illiberal-norms-russia-and-china-as-promoters-of-internet-content-control (access: 2.5.2025).

Hessoun C., *Europe: l'Armée française fait un pas vers son indépendance dans ce domaine*, 13.3.2025, https://lanouvelletribune.info/2025/03/europe-larmee-francaise-fait-un-pas-vers-son-independance-dans-ce-domaine/?utm_source=chatgpt.com#google_vignette (access: 8.4.2025).

Kempton M., Parmiggiani E., Vassilakopoulou P., *Accountability in Managing Artificial Intelligence: State of the Art and a Way Forward for Information Systems Research*, 2023, https://aisel.aisnet.org/ecis2023_rp/361 (access: 9.5.2025).

Kovachich L., Kolesnikov A., *Digital Authoritarianism with Russian Characteristics?*, 21.4.2021, https://carnegieendowment.org/posts/2021/06/digital-authoritarianism-with-russian-characteristics (access: 30.4.2025).

Ministère des Armées et des Anciens combattants, *Innovation et technologie*, https://www.defense.gouv.fr/nos-expertises/innovation-technologie (access: 2.4.2025).
NATO, *Cyber Defence*, 30.7.2024, https://www.nato.int/cps/en/natohq/topics_78170.htm (access: 2.4.2025).
NATO, *Emerging and Disruptive Technologies*, https://www.nato.int/cps/en/natohq/topics_184303.htm (access: 2.5.2025).
NATO, *Summary of the NATO Artificial Intelligence Strategy*, 22.10.2021, https://www.nato.int/cps/en/natohq/official_texts_187617.htm (access: 21.4.2025).
REMIT, *Summary of the first REMIT Conference: New Perspectives for Technology and Multilateralism, Held on May 16–17, 2024 at KU Leuven*, https://www.remit-research.eu/wp-content/uploads/2024/06/REMIT_Leuven_conference_summary_2024.pdf (access: 16.5.2025).
UNIDIR, *The Global Kaleidoscope of Military AI Governance*, 5.9.2024, https://unidir.org/publication/the-global-kaleidoscope-of-military-ai-governance (access: 30.4.2025).
Young H., *Harmonizing Cybersecurity Regulations Is a Win-Win*, 10.7.2024, https://techpost.bsa.org/2024/07/10/harmonizing-cybersecurity-regulations-is-a-win-win (access: 5.5.2025).

Legal acts

EU Artificial Intelligence Act.
EU Cyber Solidarity Act.
Regulation of the European Parliament and of the Council (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (OJ L 151/15, 7.6.2019).

ABSTRAKT

Rozwój nowych technologii, w tym sztucznej inteligencji, a także powszechne wykorzystywanie systemów teleinformatycznych przez różne podmioty, w tym odpowiedzialne za zapewnienie bezpieczeństwa militarnego, wymaga, aby szczególną uwagę zwrócić na kwestie cyberbezpieczeństwa. Cyberbezpieczeństwo zajmuje w sferze militarnej bardzo ważne miejsce, o czym świadczy również tworzenie struktur, które zajmują się tylko tą problematyką. Obroną przed zagrożeniami występującymi w cyberprzestrzeni, jako domeny operacyjnej, zajmują się też cyberwojska. Celem artykułu jest przeprowadzenie analizy dotyczącej militarnych aspektów cyberbezpieczeństwa. Jako tezę należy przyjąć stwierdzenie, że cyberbezpieczeństwo w wymiarze militarnym ma bardzo duże znaczenie dla obronności, zwłaszcza współczesnego, scyfryzowanego państwa, które musi nie tylko ponosić wydatki ze środków publicznych na zapewnienie odpowiedniej ochrony systemów teleinformatycznych wykorzystywanych w tej sferze, lecz także inwestować w kompetencje cyfrowe osób, które obsługują takie systemy. W związku z potrzebą określenia stanu badań dotyczących militarnego wymiaru cyberbezpieczeństwa została przeprowadzona analiza literatury przedmiotu. Za pośrednictwem metody dogmatyczno-prawnej określono normatywne aspekty cyberbezpieczeństwa. Obok analizy zastosowano również syntezę.

Słowa kluczowe: cyberbezpieczeństwo; siły zbrojne; nowe technologie; sztuczna inteligencja