Addressing the Legal Gaps in AI Regulation for National Security: The Case of Ukraine's Defense Sector

Submitted: 3 December 2024
Reviewed: 13 January 2025
Revised: 24 April 2025
Accepted: 26 April 2025

Oleh Semenenko[*]
https://orcid.org/0000-0001-6477-3414
Serhii Kirsanov[**]
https://orcid.org/0000-0002-9696-0369
Artur Movchan[***]
https://orcid.org/0009-0006-0559-4962
Maryna Sliusarenko[****]
https://orcid.org/0000-0003-4165-3908
Vladyslav Horhulenko[*****]
https://orcid.org/0000-0001-6382-5075

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v17i2.56351

Abstract

[Purpose] The purpose of this study was to develop a scientific and methodological framework for legal regulation of the introduction of artificial intelligence systems to ensure cybersecurity in the defense sector of Ukraine.

[Methodology] This paper evaluates the weaknesses in Ukraine's present legislation related to AI in defense cybersecurity by comparing legislative frameworks throughout the world. Based on case studies and expert interviews, it also creates a risk assessment methodology and suggests legislative changes to close these gaps.

[Findings] Thirty experts in national security, law, and cybersecurity participated in the expert survey. The study's conclusions highlight serious flaws in Ukraine's legal framework

[*]Oleh Semenenko is a Full Doctor and Deputy Head of the Institute for Scientific Work, Department of Economic Analysis of Development Measures of the Armed Forces of Ukraine, Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine. E-mail: olehsemenenko36@gmail.com.

[**]Serhii Kirsanov is a Full Doctor and Head of the Research and Development Department of Automation and Information and Communication Systems, Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine.

[***]Artur Movchan is a PhD and Head of the Research Department, Centre for Mathematical Modelling of Military and Non-military Activities, Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine.

[****]Maryna Sliusarenko is a PhD and Senior Researcher at the Research and Development Directorate for Defence Management and Development, Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine.

[*****]Vladyslav Horhulenko is a Postgraduate Student at the Scientific and Organisational Department, Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine.

for governing AI in defense cybersecurity, most notably the lack of precise definitions for autonomous cyber defense systems and AI systems. It is difficult to adequately address the hazards connected to the integration of AI technology into vital defense infrastructure because of this lack of regulatory clarity. Key legal dangers are identified by the study, including possible human rights violations such as invasions of privacy, restrictions on the right to free speech, and the possibility of discrimination. Concerns about autonomous AI systems' accountability for their deeds as well as regulatory non-compliance brought on by out-of-date or insufficient legislation are also brought to light. The paper also highlights moral conundrums that AI decision-making systems may present, which could have significant effects on both individual rights and national security. The report urges the creation of specialized law that includes precise definitions, certification procedures, accountability systems, and transparency for AI systems used in the defense industry to address these problems. These results demonstrate how urgently Ukraine must revise its legal system to guarantee that AI integration complies with contemporary technical advancements as well as the values of human rights and national security.
[Practical implications] The results of the study have considerable potential for practical application in the development of regulations and cybersecurity strategies in Ukraine, especially in the context of hybrid threats and information warfare.
[Originality] This study develops a scientific and methodological framework for the legal regulation of artificial intelligence systems to enhance cybersecurity in Ukraine's defense sector. It identifies significant gaps in Ukrainian legislation, proposes the Legal Risk Assessment Matrix to evaluate AI-related legal risks, and offers legislative recommendations, including the creation of a dedicated law on AI regulation.

Keywords: Economic Security. Cybersecurity Regulation. AI Governance. Cyber Threats. Legal System.

INTRODUCTION

Legally regulating the use of artificial intelligence (AI) in the defense industry is becoming a crucial component of national security in light of the quickening pace of technical development and the changing geopolitical landscape. For Ukraine, which is leading the charge to protect democratic principles and territorial integrity in the face of hybrid warfare and ongoing cyberthreats, this issue is especially urgent. The rapid advancement of AI technology offers previously unheard-of possibilities for improving cyber defense, but it also poses difficult problems for the legal system. It must properly balance protecting national security while respecting fundamental human rights, encouraging innovation, and guaranteeing ethical compliance. Ukraine urgently needs a flexible, all-encompassing, and efficient legal framework that is in line with contemporary technological realities, international standards, and Ukraine's particular situation as a state fending off hybrid threats (a combination of military, cyber, economic, and informational tactics used to achieve political or strategic

goals). This can be achieved by researching the legal aspects of AI deployment for securing Ukraine's defense sector.

Researchers worldwide have paid close attention to the complex role of AI in defense cybersecurity. A survey of current research indicates a variety of viewpoints and findings about this issue. The ethical ramifications of AI-driven cybersecurity systems have been discussed by M. Taddeo et al. (2019) and K. Kaushik et al. (2024), who emphasized the significance of strong governance frameworks for responsible deployment in defense contexts. Their study argued for strict control procedures and emphasized the possible risks of autonomous decision-making in critical infrastructure. Related research by H. Usman et al. (2023) looked at the legal issues raised by AI in cybersecurity, especially in developing nations and areas where geopolitical tensions are present. Their conclusions emphasized the need for an all-encompassing legal framework to handle the unique cybersecurity concerns posed by AI.

The implications of AI and machine learning in cyber intelligence were examined by A.N. Kanellopoulos (2024) and N.A. Kant (2022), who concentrated on the legal ramifications of data sharing and cross-border cooperation. In order to promote efficient cybersecurity cooperation while upholding national sovereignty, their work made clear the necessity of harmonizing international legal standards. In his analysis of the complex interrelationships among AI, cybersecurity, and international law, P. Margulies (2020) posed important queries on the suitability of current legal frameworks for dealing with AI-driven cyber operations in times of conflict. His research revealed gaps in international law that require attention and urged a reevaluation of traditional legal principles in light of emerging technologies.

In line with these discussions, J. Haner and D. Garcia (2019) investigated the moral and legal issues related to autonomous cyber capabilities, specifically those pertaining to accountability and attribution for AI-enabled cyber operations. The necessity of precise legislative frameworks controlling the application of AI in both offensive and defensive cybersecurity measures was underlined by their study. In their analysis of AI and robots in cyber risk insurance, P. Radanliev et al. (2020) highlighted the considerable difficulties in identifying and reducing the risks associated with AI-based cybersecurity systems, with consequences for the defense and national security sectors. To overcome these issues, they promoted flexible legal and regulatory frameworks.

In their analysis of AI's revolutionary potential to improve cyber resilience, S. Singh et al. (2020) offered a paradigm for incorporating AI into industrial control system security. Despite not having a clear defense industry emphasis, their study provided insightful information about the legislative obstacles to deploying AI-based security measures in critical infrastructures. A helpful

viewpoint on striking a balance between technological innovation and ethical and legal considerations was offered by N.A. Smuha's (2021) analysis of the European Union's approach to AI regulation, including its application in cybersecurity and defense. This analysis may inform Ukraine's AI governance strategy in its defense sector. Y.K. Dwivedi et al. (2021) and N. Gillespie et al. (2021) conducted a multi-country investigation into the adoption of AI in the public sector, including defense and cybersecurity. Their groundbreaking study highlighted the need for Ukraine to develop a strong, flexible legal framework and highlighted the disparities in legal readiness across nations.

There are still large gaps in the present body of study, regardless of the field's notable contributions. It has not yet been thoroughly investigated what particular legal obstacles Ukraine has when incorporating AI into defense cybersecurity. Furthermore, because technology is developing so quickly, the legal framework must be continuously assessed to guarantee its continued applicability and efficacy. Even with the amount of study done, there are still a number of important areas that are not fully understood, especially when it comes to how Ukrainian law should be adjusted to meet the difficulties posed by AI in the face of hybrid warfare and ongoing cyberthreats. A thorough strategy that tackles AI's technical potential to improve cyber defense as well as the dangers of possible abuse is desperately needed. Additionally, there is still a lack of research on international collaboration mechanisms for cybersecurity AI regulation, especially in light of Ukraine's Euro-Atlantic integration and the requirement to harmonize state laws with EU and NATO norms. Additionally, in order to enable quick legislative adaptation to new AI opportunities and problems, a system for evaluating the efficacy of legal standards in a quickly evolving technical environment must be developed.

Taking into account current technological developments, worldwide legal standards, and the unique requirements of the nation's national security, this study attempts to provide a conceptual model for the legal regulation of AI use in Ukraine's defense sector cybersecurity system. The following are the goals of this study:

• comparing and contrasting worldwide legal frameworks that govern AI in cybersecurity, with an emphasis on nations that have comparable national security issues to Ukraine;

• examining the connection between cybersecurity AI technology and Ukraine's current legal system, finding inconsistencies and gaps in the law;

• creating a framework for evaluating the legal hazards of implementing AI systems in defense cybersecurity, especially in light of information warfare (the use of information to influence, disrupt, or control through tactics like disinformation and cyberattacks) and hybrid threats;

• recommending changes to Ukrainian national law that will effectively control the use of AI in cybersecurity and include safeguards for key infrastructure and algorithm transparency.

MATERIALS AND METHODS

To provide a comprehensive and impartial examination, the research process combined general scientific techniques with specialized legal methodologies. The examination of the legal regulation of AI use in cybersecurity as a dynamic phenomenon that changes in response to technological and geopolitical circumstances was done using the dialectical method. An investigation of the connection between the elements of legal regulation and AI's technological capabilities was made easier by the systemic-structural approach. From 2019 to 2024, international practices based on laws, academic research, and official reports from international organizations were examined using the comparative legal method. NATO's practices and those of nations dealing with comparable national security issues to Ukraine were given special consideration. This analysis focused on the National Artificial Intelligence Initiative Act (NAIIA, 2020) and Regulation (EU) No. 2024/1689 of the European Parliament and Council "Laying Down Harmonized 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, as well as Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828. Legal provisions were analyzed and interpreted using the formal legal technique.

The relationship between AI's technological capabilities and Ukraine's current legal rules was investigated using the legal modelling method. Key legislative acts, including Law of Ukraine No. 2163-8 "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017), Cybersecurity Strategy of Ukraine (2021), Law of Ukraine No. 2469-8 "On National Security of Ukraine" (2018), Law of Ukraine No. 2297-6 "On Personal Data Protection" (2010), Law of Ukraine No. 3855-12 "On State Secrets" (1994), and other pertinent regulations, served as the foundation for the analysis. A methodology for evaluating the legal risks related to the deployment of AI systems in the defense industry's cybersecurity was developed by combining the legal forecasting method with risk analysis.

In order to suggest modifications to Ukraine's national legislation, the study also integrated the techniques of legal building and lawmaking experimentation. These techniques were crucial in creating certain safeguards to guarantee the security of vital infrastructure and the openness of AI algorithms. The relationship between the current legal regulations in Ukraine and the

technological capabilities of artificial intelligence in cybersecurity was visualized through a Venn diagram.

An expert survey that was carried out to verify the suggested recommendations and assess any potential legal issues was a crucial part of the study. Thirty experts participated in the survey: ten national security experts, ten cybersecurity professionals, and ten attorneys with expertise in AI legal regulation. The inclusion criteria contained publications on the research issue, at least five years of professional experience in the field, and participation in the creation of strategic documents or regulations pertaining to AI and cybersecurity. There were 20 closed-ended questions on a 5-point Likert scale, with 1 denoting "strongly disagree" and 5 denoting "strongly agree." The survey was administered using the online survey tool SurveyMonkey. The degree of consensus among experts on the legal regulation of AI in cybersecurity, possible hazards, and priority areas for legislative reforms was evaluated using this scale. Five open-ended questions were also included in the questionnaire to collect thorough feedback and recommendations. The surveys and a personal request to participate were sent to the experts via email.

A set of criteria was created to assess the identified legal concerns, taking into consideration the unique features of information warfare and hybrid threats. The probability of the risk happening and the seriousness of its effects serve as the foundation for these criteria. Making educated decisions about the deployment of AI systems in the defense industry requires the ability to evaluate each identified risk both qualitatively and quantitatively, which is made possible by this methodology.

All poll respondents provided their informed consent, which guaranteed ethical concerns. The goals of the study, the fact that participation was optional, and the fact that they might leave at any time were all explained to the experts. To ensure confidentiality, every piece of information gathered was anonymized.

RESULTS

The quick development of AI technologies and their incorporation into cybersecurity systems offer fresh chances to protect Ukraine's vital infrastructure and interests as a nation. This is especially important for the defense industry, as maintaining national security directly depends on how well cyber defense works. But the use of AI in cybersecurity also brings with it a number of legal issues that need careful consideration and handling. The legal implications of AI use in cybersecurity inside Ukraine's defense industry are the main topic of this study. It comprises a review of global regulatory standards, an assessment of how well

Ukrainian laws conform to contemporary technical advancements, and a determination of the legal concerns related to the use of AI in cyber defense.

International Practices in Regulating AI in Cybersecurity

The examination of global trends in the legislative regulation of AI usage in cybersecurity is crucial for Ukraine given the quick development of AI technologies and the rise in cyberthreats. Considering Ukraine's particular national security issues, developing a successful cyber defense strategy requires investigating and modifying the best worldwide techniques. Leading countries throughout the world are actively creating and enforcing specialized laws to control AI in cybersecurity. The National Artificial Intelligence Initiative Act (2020), for example, was passed by the United States of America (USA) and creates a framework for the advancement and application of AI, including in the field of national security. "Machine systems capable of performing tasks that normally require human intelligence" is how this statute defines artificial intelligence. The document emphasizes how crucial it is to approach AI research in a balanced manner, taking into account both the possible advantages and national security dangers. To create uniform regulations for AI within the EU, including cybersecurity considerations, the European Union has issued Regulation (EU) No. 2024/1689 of the European Parliament and of the Council (2024). A more comprehensive definition of artificial intelligence is provided by this proposed rule, which would cover systems that produce information, forecast outcomes, offer advice, or affect the environment they interact with. The European method is unique in that it clearly classifies AI systems according to their level of danger, which determines the applicable regulatory obligations.

There is no universally accepted definition of artificial intelligence across all jurisdictions. The National AI Strategy of the United Kingdom, for instance, states that AI is defined as "technologies that perform tasks that would normally require human intelligence, especially when machines are trained from data on how to perform those tasks" (Policy Paper the..., 2023). This concept is sufficiently inclusive to include a wide range of AI applications, from straightforward algorithms to intricate neural networks. On the other hand, Canadian laws emphasize AI's capacity for learning and adaptation, taking a more focused approach that targets more complex AI types. The worldwide harmonization of cybersecurity laws is hampered by the multiplicity of definitions of AI, but it also gives nations the opportunity to customize their legal systems to suit their unique requirements and legal customs.

The majority of nations identify a few primary areas for AI applications in cybersecurity: real-time cyber threat detection and response, large-scale data analysis for potential attack prediction, automation of cybersecurity procedures

like system patching and updates, and anomaly detection through user behavior and network traffic analysis. An important example is the experience of Israel, a nation that is constantly threatened by cyberattacks and is actively using AI for automated incident response and preventative attack detection. Israel's strategy is based on the idea of active defense, which uses AI to proactively identify and eliminate possible dangers in addition to providing security. Given the similarities in the security issues that both Ukraine and Russia face, Ukraine may benefit most from this experience.

Limiting the use of AI in cybersecurity is a crucial component of regulation. Numerous nations have imposed restrictions on the use of AI for mass surveillance without the required legal justification, AI decision-making in vital national security systems without human supervision, and the gathering and processing of personal data beyond what is required for cybersecurity. One notable example is Germany, where it is technically forbidden to utilize AI to identify people in public without a court order (Artificial Intelligence (AI)…, 2020). This arrangement shows an attempt to reconcile the defense of fundamental rights and freedoms with effective cyber defense. Given the continuous discussions about the moral ramifications of applying AI to national security and the requirement for public supervision of these technologies, this strategy is particularly pertinent.

The requirement for openness in AI algorithms is becoming more and more popular, especially for those employed in vital cybersecurity tasks. In this regard, public acceptability and trust are crucial for the effective deployment of AI technology in vital industries like defense. However, worries about privacy, responsibility, and the possibility of abuse are prominent reasons for skepticism and resistance toward AI, especially in delicate fields like cybersecurity. Fears that AI systems may behave opaquely or produce unfavorable results, including privacy abuses or unrestrained autonomous decision-making, frequently erode public trust. These worries are heightened in the defense industry by the alleged dangers of AI systems being applied in military or national security settings, where choices could impact on citizens' rights and safety. Thus, building public trust is crucial to the effective application of AI in these fields (Chukaieva & Matulienė, 2023).

Adopting transparent methods and having an open discussion with the public about the advantages and hazards of AI are essential to allaying public fears and fostering trust. Skepticism can be reduced by providing clear information on the moral principles, accountability procedures, and legal protections governing the application of AI in cybersecurity and defense. Furthermore, addressing issues and making sure AI systems are in line with society’s values can be achieved by including the public in decision-making processes, for example, through public

forums or consultations. Enhancing transparency can also be achieved through public-private partnerships, in which government organizations and private businesses collaborate to guarantee that AI technologies are created and used ethically. For example, developers are required to give thorough documentation on the guiding principles of AI systems used in the public sector in France. In order to preserve public confidence in the use of AI systems for national security, this criterion guarantees their accountability and auditability. Such openness also aids in identifying possible biases in AI systems that can lead to discriminatory actions or inadequate cybersecurity measures. Ukraine may promote more public acceptance and support for AI in vital areas like defense by aggressively addressing concerns and exhibiting a dedication to moral AI practices.

Another crucial topic of attention for AI cybersecurity regulation is data protection. The majority of nations impose strict regulations to reduce the amount of personal data collected, restricting it to that which is necessary for the efficient operation of cyber defense systems (Brundage et al., 2018). They also establish explicit protocols for data destruction after its intended use has been completed and require that data handled by AI systems be encrypted to avoid unwanted access. Estonia, which is renowned for its cutting-edge digital solutions, has made it necessary for all data handled by AI systems to be encrypted as part of cybersecurity (Estonia's National AI Strategy, 2019). This strategy places a strong emphasis on safeguarding private data, even in the case of a system breach. Notably, stringent data protection regulations improve cybersecurity generally and increase public confidence in government agencies that use AI. Table 1 compares the laws governing artificial intelligence in cybersecurity in various nations.

Country	Key regulations	Definition of AI	Principal areas of AI application in cybersecurity	Restrictions on the use of AI	Requirements for algorithm transparency
USA	National Artificial Intelligence Initiative Act (2020)	Systems capable of performing tasks that normally require human intelligence	Security automation, threat identification, and attack forecasting	Prohibiting the use of unwarranted mass surveillance	Algorithm documentation is required for government systems
United Kingdom	National AI Strategy (2021)	Technologies with the ability to perform tasks that normally require human intelligence	Automated response, anomaly detection, and data analysis	Limitations on vital systems' ability to make decisions on their own	Public sector AI algorithm audits on a regular basis

Germany	AI Strategy (2020)	Systems that analyze their surroundings to exhibit intelligent behavior	Preventive defense, vulnerability assessment, and network surveillance	Identification of individuals in public areas is prohibited without a court order	Algorithmic rationale and training data must be disclosed
Estonia	Estonia's National AI Strategy (2019, updated 2022)	Computer programs that can carry out operations that often call for human intelligence	Identification of cyberthreats, user behavior analysis, and critical infrastructure protection	Limitations on biometric data processing without authorization	All data handled by AI systems must be encrypted for cybersecurity purposes

Table 1 – Comparative evaluation of several nations' legal frameworks governing AI in cybersecurity

Source: created by the authors of this study based on Estonia's National AI Strategy (2019), National Artificial Intelligence Initiative Act (2020), National AI Strategy (2021), Artificial Intelligence Strategy of the German Federal Government (2020).

Table 1 illustrates how different nations have approached AI policy in cybersecurity, which makes it easier to spot both shared patterns and distinctive characteristics of each jurisdiction. This data can be used as a basis for creating legislation in Ukraine that takes into account best practices from around the world and modifies them to meet the country's unique cybersecurity requirements. Ukraine should pay particular attention to the following practices:

• the creation of specific cybersecurity AI laws that tackle Ukraine's particular security issues and provide a clear legal framework for the creation, application, and use of AI systems in this field;

• the establishment of transparent oversight procedures for the use of AI in critical infrastructure, such as a cybersecurity certification system and frequent operational audits;

• the maintenance of a balance between the effectiveness of AI systems and the defense of citizens' rights and liberties;

• the creation of specialized organizations to assess the ethical implications of applying AI in cybersecurity, guaranteeing that these technologies conform to social norms and ethical standards;

• promotion of public-private partnerships in the development and application of AI for cybersecurity, incorporating best practices from the private sector and guaranteeing quick adaptation to emerging threats.

Public-private partnerships have proven to be effective in promoting creativity and enhancing the application of AI in cybersecurity. The IndiaAI Mission, a project started by the Indian government in partnership with private

sector stakeholders, such as tech corporations and academic institutions, is one noteworthy example. Through the use of private sector resources and experience, this collaboration seeks to expedite the development of AI technologies and their applications across a range of industries, including cybersecurity. The program fosters a collaborative atmosphere that strikes a compromise between the need for rapid technology growth and regulatory compliance by emphasizing not only innovation but also regulatory frameworks, data protection, and ethical considerations. Project Maven, a partnership between the U.S. Department of Defense and many private tech firms, is another well-known example. It now supports AI and machine learning initiatives to analyze vast amounts of video data for national security objectives. This initiative demonstrates the effectiveness of public-private cooperation in tackling challenging cybersecurity and defense issues by using AI and machine learning to analyze vast amounts of video data for national security objectives.

Public-private partnerships could greatly improve the creation and application of AI-driven cybersecurity solutions in the Ukrainian setting. Through collaboration with commercial technology firms, academic institutions, and foreign partners, Ukraine might acquire the knowledge and assets required to tackle the escalating cybersecurity risks it encounters. These collaborations could hasten the creation of AI systems specifically suited for the defense industry while guaranteeing that these innovations adhere to moral and legal requirements. Given Ukraine's important position in the cybersecurity environment, where cutting-edge AI technologies might significantly increase the resilience of vital national infrastructure against cyber threats, the country has a particularly high potential for public-private partnerships. Public-private partnerships might support a strong, flexible, and safe AI ecosystem in Ukraine's cybersecurity and defense industries with the right policies and procedures in place.

Particularly crucial is the question of international collaboration in cybersecurity AI regulation. Numerous nations are actively creating bilateral and multilateral frameworks for sharing knowledge and best practices in this area, according to the report. To guarantee the security and compliance of AI systems, for example, the Cloud Security Alliance (CSA) established the AI Safety Initiative (AISI), which includes the creation of best practices and standards for the safe application of AI. By taking part in such programs, Ukraine may be able to improve its cybersecurity posture and establish itself as a major participant in the world.

It is crucial to remember that the legal regulation of AI in cybersecurity is a dynamic and changing field that adapts to the most recent developments in technology and new threats. Ukraine must not only adopt the finest worldwide standards but also create a novel strategy that fits the nation's particular security

requirements. Such an effort calls for an all-encompassing approach that includes the creation of ethical guidelines for the application of AI in national security, the development of technological infrastructure, the training of skilled workers, and legislative measures.

AI Technologies and the Legal Framework of Ukraine

The current regulatory structure in Ukraine significantly differs from the quick development of artificial intelligence technology in the cybersecurity space. In the context of cybersecurity in Ukraine, the study found several significant shortcomings in AI policy. First of all, there is no legal definition or classification of AI systems, which makes it extremely difficult to implement effective legal regulation. In particular, AI is neither defined nor categorized in relation to cybersecurity in Law of Ukraine No. 2163-8 "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017). The idea of artificial intelligence is not covered in Article 1 of this law, which defines important terminology. This underscores the absence of legal regulation for this technology in the field of cybersecurity.

The legal ambiguity around accountability for decisions made by autonomous AI systems is the second major concern. There are no explicit clauses addressing culpability for acts performed by autonomous AI systems in the present Criminal Code of Ukraine (CCU, 2001) or the Code of Administrative Offences (CAO, 1984). For example, the specifics of actions carried out by AI systems are not taken into consideration by Article 361 of the CCU, which addresses "unauthorized interference with the operation of electronic computers, automated systems, computer networks, or telecommunication networks." The lack of testing and certification guidelines for AI systems used in cybersecurity is a third serious problem. There are no particular standards for AI systems used in cybersecurity, according to an examination of the State Service for Special Communications and Information Protection of Ukraine (SSSCIP) statutory documents. The implementation of unstable technologies is made riskier by this absence.

It is advised that the aforementioned legislative acts be modified to incorporate definitions and classifications of AI, that specific laws be created to control AI in the cybersecurity industry, and that certification and testing requirements be established for AI systems utilized in cybersecurity. In addition to highlighting regulatory and technology gaps that are not currently covered by the law, the Venn diagram in Figure 1 successfully depicts the areas where technological capabilities and legal regulation coincide.

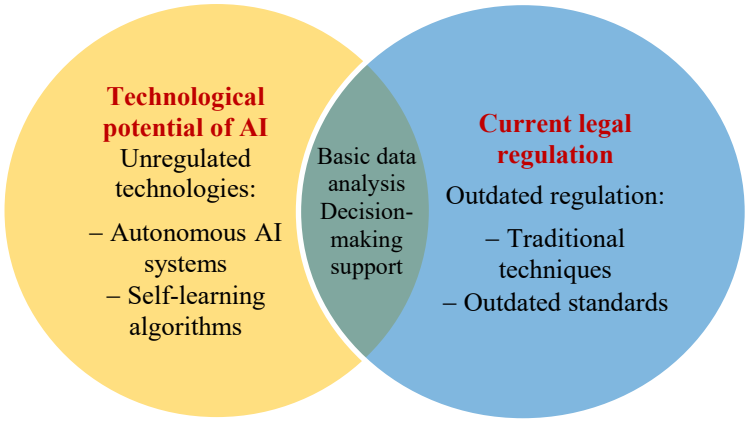

Figure 1 – Correlation of AI technological capabilities and legal regulation in Ukraine
Source: created by the authors of this study based on O. Baranov et al. (2024).

The technological potential of artificial intelligence and Ukraine's current legislative framework were found to be significantly at odds. In particular, the regulatory framework does not address the use of self-learning algorithms and autonomous AI systems in cybersecurity. Legally speaking, this poses possible threats to national security and could result in the defense industry using cutting-edge technologies inefficiently. On the other hand, some of the current laws are based on antiquated practices and guidelines that do not take into consideration AI's current capabilities. This emphasizes how urgently the cybersecurity regulatory framework has to be updated to reflect modern technological realities.

The study also found unresolved problems with protecting personal data while analyzing cyber threats with AI. The processing of personal data by AI systems in the area of cybersecurity is not specifically covered under Law of Ukraine No. 2297-6 “On Personal Data Protection” (2010). Legally speaking, this calls for changes to the laws protecting personal data in order to create unique guidelines and protections for data processing by AI systems employed for cybersecurity.

Ukrainian laws urgently need to be modified to handle the difficulties brought on by the application of AI in cybersecurity. A thorough legal framework should be created to specify the legal standing of AI systems in cybersecurity, assign precise accountability for autonomous systems' actions, control data collection and processing by AI systems in accordance with regulations pertaining to the protection of personal data, and implement certification and quality control procedures for AI systems in cybersecurity. Integrating ethical concepts about AI

in cybersecurity into the legal system is another crucial element. This could be accomplished by enacting legislation specifically addressing AI's application in cybersecurity or by making the necessary changes to current laws.

Numerous nations have already started modifying their laws to address the difficulties presented by artificial intelligence in cybersecurity, according to an examination of global experience. As Ukraine creates its own regulatory framework, it can benefit from the EU's experience in creating a thorough regulatory approach to AI that takes cybersecurity concerns into account. Ukraine's unique needs, especially those of the defense industry and current cyberthreats, must be taken into consideration when designing this framework. To do this, more investigation and discussions with legal, AI, and cybersecurity specialists will be required to create fair and efficient legislative frameworks for controlling AI use in cybersecurity in Ukraine.

Assessment of the Legal Risks of AI in Defense Cybersecurity

A number of legal dangers are associated with the integration of AI systems into Ukraine's defense industry's cybersecurity, which calls for careful consideration and methodical planning. Human rights risks, liability risks, regulatory non-compliance risks, international law risks, and ethical risks are the main types of legal risks in this situation. Each of these groups has a wide range of possible legal problems that require careful analysis and deliberation.

When AI is used in defense cybersecurity, the concerns about human rights, such as non-discrimination, freedom of expression, and privacy, become even more serious. AI systems may violate the right to privacy protected by Article 8 of the European Convention on Human Rights (1950) by processing vast amounts of personal data. Furthermore, AI systems created to identify dangers may excessively restrict the right to free speech, which is guaranteed by Article 10 of the European Convention, or encourage prejudice against particular groups, which is prohibited by Article 14. The proportionality principle is essential in this situation since any restriction on rights must be both required and consistent with a justifiable purpose.

Liability risks pose significant legal difficulties, especially when it comes to assigning blame for mistakes or malfunctions of AI systems. These risks are particularly significant in the defense industry, where mistakes of this nature could have a significant impact on national security. To reduce this risk, it is crucial to specify precisely what the roles of AI developers, operators, and end users are. Legally speaking, the situation necessitates the development of particular laws that address the special features of AI and its use in the defense industry; this strategy is backed by the European Commission's recommendations on the legal regulation of AI (Proposal for a Regulation…, 2021).

Potential conflicts between the activities of AI systems and current legal regulations give rise to regulatory non-compliance issues. The requirement to adhere to both national legislation and international cybersecurity and information protection requirements exacerbates this problem in the defense industry. AI system compliance with the provisions of Law of Ukraine No. 2297-6 "On Personal Data Protection" (2010) and Law of Ukraine No. 3855-12 "On State Secrets" (1994) should receive particular attention. Legal examination of these concerns indicates that particular legislation with well-defined standards for information and personal data protection must be developed to control the use of AI in the defense industry.

The difficulties that result from competing agendas, such as the friction between the need for transparency and military secrecy needs, should be taken into account when examining the possible obstacles to cooperation among stakeholders. The successful development and application of AI in cybersecurity depend on cooperation between the government, military, private sector businesses, and academic institutes; yet, military secrecy frequently poses a major barrier (Striltsiv & Fedorenko, 2022; Dashkovska, 2023). The requirement for transparency in AI systems, which is essential for maintaining public confidence and accountability, may clash with the necessity to protect sensitive defense data. Developing techniques that strike a compromise between national security concerns and the transparency necessary for effective AI regulation is essential to overcoming this. Such an endeavor could entail setting up safe routes of communication, outlining precise rules for exchanging information, and developing supervision procedures that guarantee privacy and openness.

The possibility of breaking international defense and cybersecurity accords and conventions is one of the hazards associated with international law. The autonomous acts of AI systems may violate international cyberwarfare regulations or international humanitarian law principles, especially those specified in the Geneva Conventions and their Additional Protocols, if AI is used in the defense industry. The necessity of creating international norms and regulations for the application of AI in the military and the significance of incorporating AI clauses into current international cybersecurity agreements are both highlighted by the legal evaluation of these concerns.

In the context of cybersecurity in the defense industry, ethical risks (especially those resulting from possible ethical quandaries in AI systems' decision-making) are particularly important. AI decisions have the potential to seriously affect national security, human life, and health.

Risk identification, qualitative risk assessment, quantitative risk assessment, risk ranking, and suggestion formulation are the five primary steps of the legal risk assessment technique created in this study. This methodology's main

tool, the Matrix for Assessing Legal hazards of AI Implementation in Cybersecurity, aids in the analysis and visualization of the hazards that have been discovered (Table 2). The most significant danger, according to this matrix, is the possible infringement of human rights, especially freedom of expression, when an AI system is used to identify and combat misinformation in Ukraine's defense industry. This emphasizes the necessity of striking a balance between the defense of fundamental human rights and national security considerations, in accordance with the guidelines set forth in European Court of Human Rights (ECtHR) decisions. A worry that is closely related to the use of AI in cybersecurity is the necessity of developing clear and predictable regulations for the bulk interception of communications, as the court stressed in the case of Big Brother Watch and Others v. the United Kingdom (Zalnieriute, 2022). Furthermore, the court in the Case of Centrum för Rättvisa v. Sweden (2021) emphasized the necessity of efficient supervision and management of mass surveillance systems, which is an essential factor for the application of AI in the defense industry.

Risk category	**Risk description**	**Probability (1-5)**	**Severity of consequences (1-5)**	**General risk assessment**	**Possible measures of protest**
Human rights violations	Excessive content screening that unlawfully restricts the right to free speech	4	5	20	Creation of precise filtering standards, frequent system audits, and a procedure for judgement appeals
Risk of liability	Finding the accountable party can be challenging if the AI system incorrectly detects a threat	3	4	12	Establishing a shared responsibility framework and requiring risk insurance
Regulatory non-compliance	AI algorithms and the obligations of laws protecting personal data are at odds	5	3	15	Creation of specific laws pertaining to the application of AI in the defense industry and discussions with legal professionals
International law	Possible breach of global cybersecurity accords as a	2	5	10	Application of global standards in the realm of AI and ongoing oversight of

	result of an AI system acting on its own				adherence to international law
Ethical risks	AI systems that make choices that go against societal standards	3	4	12	Establishing an ethical commission to supervise the application of AI and developing a code of ethics for AI systems

Table 2 – A matrix for evaluating the legal risks associated with integrating AI into cybersecurity

Note: This matrix's overall risk score is determined by multiplying the Probability of Risk Occurrence by the Consequences Severity. The ratings for both of these parameters range from 1 to 5, with 5 representing the highest value and 1 representing the lowest.
Source: created by the authors.

The legal analysis technique created to analyze the dangers of integrating AI into the defense industry's cybersecurity demonstrates how promising it is as a tool for preventive legal control. Mandatory legal evaluations of AI systems before they are implemented in vital infrastructure could be based on this concept. Administratively speaking, it might be put into practice by requiring AI systems in the defense industry to be certified. This would provide a legal framework that would guarantee AI technologies adhere to regulations while they are being developed.

The methodology could serve as the foundation for the creation of a new category of "information and algorithmic security" in the field of information law, which would address the dangers associated with AI systems' autonomy. From the perspective of constitutional law, its implementation would help strike a balance between the preservation of human rights and national security objectives by offering a way to evaluate such infractions. In terms of international law, this approach may serve as a foundation for the creation of guidelines for evaluating the risks associated with AI in the military setting, which would help to standardize the ways in which various nations regulate this technology.

Proposals for the Adaptation of Ukrainian Legislation on AI in Cybersecurity

It has been determined that Ukraine's national laws urgently need to be modified in order to properly control the application of AI in defense cybersecurity. Legal regulation faces new difficulties as a result of the quick development of AI technology and its application in cybersecurity. Given the current geopolitical climate and growing cyberthreats, this topic is especially

important in the Ukrainian context. A thorough strategy that takes into account both the technical and moral aspects of these technologies is necessary for the effective legal regulation of AI in cybersecurity.

The following changes are suggested to certain Ukrainian legislation and regulations. Definitions of "artificial intelligence systems in cybersecurity" and "autonomous cyber defense systems" should be included in Article 1 of Law of Ukraine No. 2163-8, "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017). Modern international standards, especially those established by the Organization for Economic Co-operation and Development (OECD, 2019), should be reflected in these definitions. It is also suggested that an article discussing the particulars of AI application in critical infrastructure cyber defense systems be included in Section II. It is suggested that Article 6 of Law of Ukraine No. 2297-6 "On Personal Data Protection" (2010) be amended to reflect the particulars of AI systems' processing of personal data in relation to cybersecurity. It is also suggested that a provision outlining the rights of individuals with personal data with regard to decisions made by automated AI systems is added to the law. It is essential to guarantee human control over computerized decision-making systems. The definition of "threat to national security in the field of AI" should be included in Article 1 of Law of Ukraine No. 2469-8 "On National Security of Ukraine" (2018). This definition should take into consideration the threats of AI being misused by bad actors as well as the concerns of Ukraine's lack of AI development, which could lead to a cybersecurity technology gap. It is also advised that Section III be changed to incorporate clauses pertaining to a plan for the advancement and use of AI in the national security system. Both offensive and defensive applications of AI in cyberspace should be covered by this plan.

The Law of Ukraine "On Regulation of Artificial Intelligence in the Field of National Security and Defense" is one example of a suggested new regulatory statute. A legal framework for the development, testing, and deployment of AI systems in the defense industry should be established by this law, which should also define key concepts, categorize AI systems, control accountability for AI decisions, and provide procedures for monitoring and auditing AI systems in critical infrastructure. Adopting a Resolution from the Ukrainian Cabinet of Ministers (CMU) titled "On the Procedure for Certification of Artificial Intelligence Systems for Use in Cybersecurity" is also advised. The authorized certification authority should be named, the certification criteria and procedures should be established, and the procedures for routine audits of certified systems should be regulated. It would be wise to take into account EU procedures for setting up an AI certification system while creating this resolution.

An "explainable AI" approach for crucial decision-making systems is suggested to guarantee the openness of AI algorithms in the context of national

security. It is essential to comprehend how AI systems make decisions in order to maintain responsibility and confidence. Establishing a registry of AI algorithms utilized in cybersecurity systems of national importance and establishing guidelines for recording these AI systems' decision-making processes are also advised.

Transparency, accountability, and justice must be given top priority in particular systems and frameworks that guarantee adherence to ethical standards in the defense industry's use of AI. The EU's Ethics Guidelines for Trustworthy AI is one such framework that provides important guidelines for the creation and application of AI systems, such as making sure AI is open, responsible, and human rights-compliant. To foster confidence, these principles stress how crucial it is that AI systems be built with explicable design and transparent documentation of decision-making procedures. These moral precepts can be modified for the Ukrainian context by being incorporated into national laws, especially those pertaining to the defense industry. This might entail setting up a national AI ethics council formed out of independent ethicists, legal professionals, and military officials to supervise the use of AI in defense cybersecurity.

It is suggested that a technique for evaluating the risks of integrating AI into critical infrastructure protection systems be developed in order to improve the legal protection of critical infrastructure when utilizing AI. Both the technological and socioeconomic facets of implementing AI should be covered by this methodology. Along with backup control mechanisms to deal with malfunctions in the operation of autonomous AI systems, it is also advised to set up a system for the early identification and response to anomalies in the operation of AI systems in critical infrastructure.

A thorough framework for regulating AI in cybersecurity in Ukraine should be established by the suggested changes to current laws and the development of new rules. Their deployment will guarantee the protection of people's rights and national interests in the digital sphere and increase the efficacy of AI in the defense industry. The legislative adaptation procedure should, therefore, continue to be adaptable in order to take into account the quick advancement of AI technology. Regulation of AI should combine promoting innovation with reducing dangers, especially when it comes to cybersecurity and national security.

DISCUSSION

The study's findings on the legal implications of utilizing AI to guarantee cybersecurity in Ukraine's defense industry highlight a number of significant problems and opportunities that call for careful consideration and debate in light of international developments and research. The observed discrepancy between

Ukraine's current legislative structure and the swift advancement of AI technology is not specific to this nation; rather, it is a prevalent problem in many nations. The results of M. Taddeo et al. (2021), who draw attention to the worldwide issue of a "regulatory gap" in AI and cybersecurity, support this. In line with the findings about the need to update Ukrainian legislation, the researchers stress the importance of creating adaptable legal systems that can keep up with the quick changes in technology. But the report also reveals problems unique to Ukraine, like the absence of a legal framework for artificial intelligence in cybersecurity and the open questions around accountability for autonomous system behavior. These concerns are especially important given the increasing cyberthreats to Ukraine's defense industry.

M. Paterra (2021) supported the suggested methodology for evaluating the legal risks related to the integration of AI into cybersecurity, emphasizing the significance of a methodical approach to risk assessment in critical infrastructures. The approach suggested by these researchers is in line with the risk assessment matrix, which comprises categories like responsibility, international law, human rights breaches, regulatory non-compliance, and ethical considerations. However, the study expands on this strategy by tailoring it to the unique requirements of Ukraine's defense industry while concentrating on legal issues. This modification offers a more accurate risk assessment in relation to cybersecurity and national security. N.A. Smuha (2021) confirms the concerns of human rights breaches associated with AI's application in cybersecurity, including possible discrimination and limitations on freedom of expression. In line with the suggestions for putting control and audit mechanisms for AI systems in critical infrastructure in place, the researcher highlights the significance of striking a balance between the protection of fundamental rights and the effectiveness of AI systems. The study broadens this conversation by looking at these vulnerabilities in the particular context of Ukraine's defense industry, where it can be difficult to strike a balance between protecting human rights and maintaining national security.

The suggested changes to Ukrainian law are supported by C. Cath et al. (2020), especially the addition of definitions of AI and autonomous cyber defense systems to pertinent legislation. The researchers stress how crucial precise legal definitions are to the efficient control of AI in vital industries. This paper develops this concept by suggesting precise language and implementation procedures for Ukrainian law, which could act as a template for other nations dealing with comparable issues. The findings of K. Brockmann et al. (2019), who emphasize the necessity of a unique legal framework for the military use of AI, are consistent with the stated need for specialized legislation governing AI in the defense sector. The report goes one step further by suggesting a specific structure for such laws

in Ukraine, along with procedures for AI system certification and audits. The recommendations could have a major impact on how international legislation governing military AI technologies develops.

S. Robbins (2020) backs up recommendations for using explainable AI in important decision-making systems, stressing the significance of algorithm transparency to guarantee accountability and confidence. The report expands on this idea by suggesting workable implementation strategies for cybersecurity in Ukraine's defense sector, such as the establishment of a registry of AI algorithms and specifications for recording decision-making procedures. The problems with protecting personal data when using AI to assess cyberthreats align with the conclusions of A. Tsamados et al. (2022), who support the creation of certain guidelines for AI data processing in the interest of national security.

V. Dignum (2019) supports the idea of "information and algorithmic security" as a new category in information law, emphasizing the necessity of broadening legal terms to more accurately reflect the reality of AI. The conclusions of M.N. Schmitt (2020), who advocates for changes to current international standards in light of new technology, are consistent with the need to adapt international law to the difficulties brought by AI in cybersecurity. By suggesting particular areas for international cooperation on AI regulation in the defense sector, the study expands on this conversation and may be a useful addition to the evolution of international cybersecurity law.

The significance of a proactive approach to AI risk management is emphasized by B. Perry and R. Uuk (2019), who endorse the recommendations for developing a system for early detection and response to anomalies in AI systems in critical infrastructure. The report expands on this concept by suggesting specific implementation strategies for cybersecurity in Ukraine's defense industry. The findings of L. Floridi et al. (2018), who stress the significance of "ethical design" in AI systems, are compatible with the necessity of striking a balance between innovation and risk mitigation in AI regulation. By suggesting specific legislative measures to guarantee the moral application of AI in cybersecurity, such as the creation of ethics committees and codes of ethics, the study supports this idea.

The need for collaboration between the public and commercial sectors in creating secure AI systems is emphasized by M. Brundage et al. (2020), who support the ideas for implementing public-private partnership frameworks in the development of AI for cybersecurity. The paper expands on this concept by suggesting certain legal frameworks for this kind of collaboration within the framework of Ukraine's defense industry. The necessity to align national laws with EU and NATO norms and Ukraine's Euro-Atlantic integration make this issue especially pertinent. I. Ulnicane et al. (2022), who examined patterns in

global collaboration on AI regulation, support these findings. Coordination is necessary for effective AI regulation in today's globalized society, especially in delicate fields like defense and cybersecurity.

The importance of preventive legal regulation for AI is emphasized by K. Yeung et al. (2019), who endorse recommendations for required legal expertise of AI systems before their deployment in critical infrastructure. The report suggests specific procedures for this kind of cybersecurity competence in Ukraine's defense industry. The findings of J. Mökander and M. Axente (2023), who emphasize the need for an interdisciplinary approach to AI governance, are consistent with the stated need for specialized education and training in the legal regulation of AI in cybersecurity. By suggesting certain paths for the development of training and educational initiatives in Ukraine, the study expands on this idea.

The work by M. Horowitz and P. Scharre (2021), which addresses strategic stability in the context of AI in the defense industry, is also noteworthy. In order to avoid disputes brought on by mistakes or misunderstandings of AI systems, the researchers emphasize the necessity of creating international norms. Discussing the geopolitical ramifications of AI technology, this work contributes a significant dimension to the legal concerns of AI in cybersecurity. The topic of legal regulation of AI in cybersecurity is further discussed by J.M. Schraagen (2023), who focuses on liability for harm produced by autonomous systems. The researcher offers a fresh definition of accountability that takes into account the intricacy of interactions between humans and machines during decision-making. By highlighting the necessity of taking into account the particular features of autonomous systems when assessing legal culpability, this study supports the case for creating specialized legislation to regulate AI in the defense industry.

In conclusion, the study's findings not only support the opinions of many international experts regarding the significance of modifying laws to address the difficulties presented by artificial intelligence in cybersecurity, but they also offer fresh perspectives by providing Ukraine with specific mechanisms and suggestions. Notably, Ukraine and other nations dealing with comparable difficulties in regulating AI in the defense industry may benefit from the study's contribution to the creation of a methodology for evaluating the legal risks of AI in the context of national security as well as suggestions for amending Ukrainian law. Simultaneously, the study has identified areas that need more research, such as effective auditing and control systems for AI in critical infrastructures and

methods for the worldwide harmonization of AI legal legislation. Future studies in this significant and ever-evolving topic may build on these themes.

CONCLUSIONS

The study identified key aspects of legal regulation of the use of AI to ensure cybersecurity of the Ukrainian defense sector and developed a conceptual model of such regulation. A comparative analysis of international experience revealed the absence of a unified universal approach to the legal definition of AI and its regulation in the context of cybersecurity. It was found that key world powers, namely the USA, EU countries, and the UK, are actively developing specialized legislation on AI, considering its application in the defense sector. The key areas of regulation include detecting and responding to cyberthreats, predicting attacks, automating protection, and analyzing user behavior. The experience of Israel, which is based on the concept of active defense using AI to proactively detect and neutralize potential threats, proved to be particularly valuable for Ukraine.

A study of the relationship between AI technological capabilities and the existing legal framework in Ukraine revealed substantial gaps in regulation. The study noted the absence of a legislative definition and classification of AI systems, uncertainty about the responsibility for the decisions of autonomous systems, and the lack of AI certification standards for cybersecurity. This creates risks of inefficient use of advanced technologies and potential threats to national security. The analysis of the current legislation indicated that it does not contain special provisions for regulating AI in the context of cybersecurity, which creates legal uncertainty and potential risks to the rights of citizens.

The methodology for assessing the legal risks of introducing AI into cybersecurity developed during the study includes five stages: identification, qualitative assessment, quantitative assessment, risk ranking, and development of recommendations. The key tool was the Legal Risk Assessment Matrix, which helped to identify the most critical risk of human rights violations, including freedom of expression. Applying this matrix to the example of assessing the risk of implementing an AI system to detect and counter disinformation in the defense sector of Ukraine showed that the probability of this risk occurring is estimated at 4 points out of 5, and the severity of the consequences is estimated at 5 points out of 5, which gives an overall risk score of 20 points – the highest among all the risks assessed.

The study formulated concrete proposals for the adaptation of Ukrainian legislation. Specifically, it is recommended to amend the current legislation regulating the use of AI. Accordingly, it is proposed to develop a new law, "On the Regulation of Artificial Intelligence in the Field of National Security and

Defense," and a Cabinet of Ministers of Ukraine resolution on the certification of AI systems for cybersecurity. These legislative initiatives are aimed at creating a comprehensive system of legal regulation of AI in Ukraine's cybersecurity, which will not only increase the efficiency of AI use in the defense sector but also ensure proper protection of citizens' rights and national interests in the digital space.

The limitations of this study are related to the dynamic development of AI technologies, which may require constant updating of legal norms, as well as the difficulty of predicting all potential risks of using AI in cybersecurity. Further research should focus on developing mechanisms for implementing the proposed legislative changes, conducting interdisciplinary research at the intersection of law, information technology, and national security, and exploring opportunities for international cooperation in regulating AI for cybersecurity.

The findings obtained can be applied in the development of regulations and cybersecurity strategies in Ukraine. The proposed conceptual model of legal regulation of the use of AI in the cybersecurity system of the defense sector of Ukraine considers modern technological capabilities, international legal norms, and the specifics of the country's national security, which makes it particularly valuable in the context of hybrid threats and information warfare faced by Ukraine.

DECLARATION OF CONFLICTING INTERESTS

The authors declare that they have no existing or potential conflicting interests with respect to the research, authorship and publication of this paper.

FUNDING

The authors received no financial support for the research, authorship and/or publication of this paper.

REFERENCES

Artificial Intelligence (AI) is a Key to the World of Tomorrow. (2020). https://www.ki-strategie-deutschland.de/files/downloads/Fortschreibung_KI-Strategie_engl.pdf

Artificial Intelligence Strategy of the German Federal Government. (2020). https://www.ki-strategie-deutschland.de/files/downloads/Fortschreibung_KI-Strategie_engl.pdf

BARANOV, O., KOSTENKO, O., DUBNIAK, M., & GOLOVKO, O. (2024). *Digital Transformations of Society: Problems of Law.* RS Global. https://doi.org/10.31435/rsglobal/057

BROCKMANN, K., BAUER, S., & BOULANIN, V. (2019). *Bio plus X: Arms Control and the Convergence of Biology and Emerging Technologies.* Stockholm International Peace Research Institute.

BRUNDAGE, M., AVIN, S., CLARK, J., TONER, H., ECKERSLEY, P., GARFINKEL, B., DAFOE, A., SCHARRE, P., ZEITZOFF, T., FILAR, B., ANDERSON, H., ROFF, H., ALLEN, G.C., STEINHARDT, J., FLYNN, C., HÉIGEARTAIGH, S.Ó., BEARD, S., BELFIELD, H., FARQUHAR, S., LYLE, C., CROOTOF, R., EVANS, O., PAGE, M., BRYSON, J., YAMPOLSKIY, R., & AMODEI. D. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.* Apollo – University of Cambridge Repository. https://doi.org/10.17863/CAM.22520

BRUNDAGE, M., AVIN, S., WANG, J., BELFIELD, H., KRUEGER, G., HADFIELD, G., KHLAAF, H., YANG, J., TONER, H., FONG, R., MAHARAJ, T., KOH, P.W., HOOKER, S., LEUNG, J., TRASK, A., BLUEMKE, E., LEBENSOLD, J., O'KEEFE, C., KOREN, M., RYFFEL, T., RUBINOVITZ, JB., BESIROGLU, T., CARUGATI, F., CLARK, J., ECKERSLEY, P., DE HAAS, S., JOHNSON, M., LAURIE, B., INGERMAN, A., KRAWCZUK, I., ASKELL, M., CAMMAROTA, R., LOHN, A., KRUEGER, D., STIX, C., HENDERSON, P., GRAHAM, L., PRUNKL, C., MARTIN, B., SEGER, E., ZILBERMAN, N., HÉIGEARTAIGH, S.Ó., KROEGER, F., SASTRY, G., KAGAN, R., WELLER, A., TSE, B., BARNES, E., DAFOE, A., SCHARRE, P., HERBERT-VOSS, A., RASSER, M., SODHANI, S., FLYNN, C., GILBERT, T.K., DYER, L., KHAN, S., BENGIO, Y., & ANDERLJUNG, M. (2020). *Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims.* https://arxiv.org/pdf/2004.07213

Case of Centrum för Rättvisa v. Sweden. (2021). https://hudoc.echr.coe.int/fre#{%22sort%22:[%22kpdate%20Descending%22],%22itemid%22:[%22001-210078%22]}

CATH, C., WACHTER, S., MITTELSTADT, B., TADDEO, M., & FLORIDI, L. (2020). Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach. *Science and Engineering Ethics,* 24(2), 505-528. https://doi.org/10.1007/s11948-017-9901-7

CHUKAIEVA, A., & MATULIENĖ, S. (2023). Possibilities of applying artificial intelligence in the work of law enforcement agencies. *Scientific Journal of the National Academy of Internal Affairs*, 28(3), 28-37. https://doi.org/10.56215/naia-herald/3.2023.28.

Criminal Code of Ukraine. (2001). https://zakon.rada.gov.ua/laws/show/2341-14#Text

Cybersecurity Strategy of Ukraine. (2021). https://cip.gov.ua/ua/news/strategiya-kiberbezpeki-ukrayini

DASHKOVSKA, A. (2023). National security and defense council of Ukraine: Administrative and legal status. *Law Journal of the National Academy of Internal Affairs*, 13(1), 53-62. https://doi.org/10.56215/naia-chasopis/1.2023.53.

DIGNUM, V. (2019). *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way.* Springer. https://doi.org/10.1007/978-3-030-30371-6

DWIVEDI, Y.K., HUGHES, L., ISMAGILOVA, E., AARTS, G., COOMBS, C., CRICK, T., DUAN, Y., DWIVEDI, R., EDWARDS, J., EIRUG, A., GALANOS, V., ILAVARASAN, P.V., JANSSEN, M., JONES, P., KAR, A.K., KIZGIN, H., KRONEMANN, B., LAL, B., LUCINI, B., MEDAGLIA, R., & WILLIAMS, M.D. (2021). Artificial Intelligence (AI): Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy. *International Journal of Information Management*, 57, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Estonia's National AI Strategy. (2019). https://ai-watch.ec.europa.eu/countries/estonia/estonia-ai-strategy-report_en#ecl-inpage-249

European Convention on Human Rights. (1950). https://zakon.rada.gov.ua/laws/show/995_004#Text

FLORIDI, L., COWLS, J., BELTRAMETTI, M., CHATILA, R., CHAZERAND, P., DIGNUM, V., LUETGE, C., MADELIN, R., PAGALLO, U., ROSSI, F., SCHAFER, B., VALCKE, P., & VAYENA, E. (2018). AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, 28(4), 689-707. https://doi.org/10.1007/s11023-018-9482-5

GILLESPIE, N., LOCKEY, S., & CURTIS, C. (2021). *Trust in Artificial Intelligence: A Five Country Study.* University of Queensland, KPMG Australia. https://doi.org/10.14264/e34bfa3

HANER, J., & GARCIA, D. (2019). The Artificial Intelligence Arms Race: Trends and World Leaders in Autonomous Weapons Development. *Global Policy*, 10(3), 331-337. https://doi.org/10.1111/1758-5899.12713

HOROWITZ, M., & SCHARRE, P. (2021). *AI and International Stability: Risks and Confidence-Building Measures*. Center for a New American Security. https://www.cnas.org/publications/reports/ai-and-international-stability-risks-and-confidence-building-measures.

KANELLOPOULOS, A.N. (2024). Counterintelligence, Artificial Intelligence and National Security: Synergy and Challenges. *Journal of Politics and Ethics in New Technologies and AI*, 3(1), e35617. https://doi.org/10.12681/jpentai.35617

KANT, N.A. (2022). How Cyber Threat Intelligence (CTI) Ensures Cyber Resilience Using Artificial Intelligence and Machine Learning. In J.O. PRAKASH, H.L. GURURAJ, & M.R. POOJA (Eds.), *Methods, Implementation, and Application of Cyber Security Intelligence and Analytics* (pp. 65-96). IGI Global. https://doi.org/10.4018/978-1-6684-3991-3.ch005

KAUSHIK, K., KHAN, A., KUMARI, A., SHARMA, I., & DUBEY, R. (2024). Ethical Considerations in AI-Based Cybersecurity. In K. KAUSHIK, & I. SHARMA (Eds.), *Next-Generation Cybersecurity. Blockchain Technologies* (pp. 437-470). Springer. https://doi.org/10.1007/978-981-97-1249-6_19

Law of Ukraine No. 2163-8 "On the Basic Principles of Ensuring Cybersecurity of Ukraine". (2017). https://zakon.rada.gov.ua/laws/show/2163-19#Text.

Law of Ukraine No. 2297-6 "On Personal Data Protection". (2010). https://zakon.rada.gov.ua/laws/show/2297-17#Text

Law of Ukraine No. 2469-8 "On National Security of Ukraine". (2018).http://zakon.rada.gov.ua/laws/show/2469-19.

Law of Ukraine No. 3855-12 "On State Secrets". (1994). https://zakon.rada.gov.ua/laws/show/3855-12#Text

MARGULIES, P. (2020). Autonomous Cyber Capabilities below and above the Use of Force Threshold: Balancing Proportionality and the Need for Speed. *International Law Studies*, 96, 395-441.

MÖKANDER, J., & AXENTE, M. (2023). Ethics-Based Auditing of Automated Decision-Making Systems: Intervention Points and Policy Implications. *AI & Society*, 38(1), 153-171. https://doi.org/10.1007/s00146-021-01286-x

National AI Strategy. (2021). https://www.gov.uk/government/publications/national-ai-strategy

National Artificial Intelligence Initiative Act. (2020). https://www.congress.gov/bill/116th-congress/house-bill/6216

OECD. (2019). *Recommendation of the Council on Artificial Intelligence.* https://oecd.ai/en/assets/files/OECD-LEGAL-0449-en.pdf

PATERRA, M. (2021). *Artificial Intelligence & Cybersecurity: Balancing Innovation, Execution and Risk.* https://impact.economist.com/perspectives/technology-innovation/artificial-intelligence-cybersecurity-balancing-innovation-execution-and-risk

PERRY, B., & UUK, R. (2019). AI Governance and the Policymaking Process: Key Considerations for Reducing AI Risk. *Big Data and Cognitive Computing,* 3(2), 26. https://doi.org/10.3390/bdcc3020026

Policy Paper the UK's International Technology Strategy. (2023). https://www.gov.uk/government/publications/uk-international-technology-strategy/the-uks-international-technology-strategy

Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

RADANLIEV, P., DE ROURE, D., WALTON, R., VAN KLEEK, M., MONTALVO, R.M., MADDOX, L.T., SANTOS, O., BURNAP, P., & ANTHI, E. (2020). Artificial Intelligence and Machine Learning in Dynamic Cyber Risk Analytics at the Edge. *Discover Applied Sciences,* 2, 1773. https://doi.org/10.1007/s42452-020-03559-4

Regulation (EU) No. 2024/1689 of the European Parliament and of the Council "Laying Down Harmonized Rules on Artificial Intelligence and Amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) No. 2018/858, (EU) No. 2018/1139 and (EU) No. 2019/2144 and Directives No. 2014/90/EU, (EU) 2016/797 and (EU) No. 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). (2024). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

ROBBINS, S. (2020). AI and the Path to Envelopment: Knowledge as a First Step Towards the Responsible Regulation and Use of AI-powered Machines. *AI & Society*, 35(2), 391-400. https://doi.org/10.1007/s00146-019-00891-1

SCHMITT, M.N. (2020). Autonomous Cyber Capabilities and the International Law of Sovereignty and Intervention. *International Law Studies,* 96, 549-578.

SCHRAAGEN, J.M. (2023). Responsible Use of AI in Military Systems: Prospects and Challenges. *Ergonomics*, 66(11), 1719-1729. https://doi.org/10.1080/00140139.2023.2278394

SINGH, S., KARIMIPOUR, H., HADDADPAJOUH, H., & DEHGHANTANHA, A. (2020). Artificial Intelligence and Security of Industrial Control Systems. In: K.K. CHOO, & A. DEHGHANTANHA (Eds.), *Handbook of Big Data Privacy* (pp. 121-164). Springer. https://doi.org/10.1007/978-3-030-38557-6_7

SMUHA, N.A. (2021). From a 'Race to AI' to a 'Race to AI regulation' – Regulatory competition for artificial intelligence. *Published in Law, Innovation and Technology*, 13(1). https://dx.doi.org/10.2139/ssrn.3501410

STRILTSIV, O., & FEDORENKO, O. (2022). Problems of legal regulation of the use of artificial intelligence technologies by the National police of Ukraine. *Scientific Journal of the National Academy of Internal Affairs*, 27(1), 30-39. https://doi.org/10.56215/0122271.30.

TADDEO, M., MCCUTCHEON, T., & FLORIDI, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, 1(12), 557-560. https://doi.org/10.1038/s42256-019-0109-1

TADDEO, M., MCNEISH, D., BLANCHARD, A., & EDGAR, E. (2021). Ethical principles for artificial intelligence in national defence. *Philosophy & Technology,* 34(4), 1707-1729. https://doi.org/10.1007/s13347-021-00482-3

TSAMADOS, A., AGGARWAL, N., COWLS, J., MORLEY, J., ROBERTS, H., TADDEO, M., & FLORIDI, L. (2022). The Ethics of Algorithms: Key Problems and Solutions. *AI & Society,* 37(1), 215-230. https://doi.org/10.1007/s00146-021-01154-8

ULNICANE, I., KNIGHT, W., LEACH, T., STAHL, B.C., & WANJIKU, W.G. (2022). Governance of Artificial Intelligence: Emerging International Trends and Policy Frames. In T. MAURIZIO (Ed.), *The Global Politics of Artificial Intelligence* (pp. 29-55). Chapman and Hall/CRC.

USMAN, H., NAWAZ, B., & NASEER, S. (2023). The Future of State Sovereignty in the Age of Artificial Intelligence. *Journal of Law & Social Studies*, 5(2), 142-152.

YEUNG, K., HOWES, A., & POGREBNA, G. (2019). AI Governance by Human Rights-Centred Design, Deliberation and Oversight: An End to Ethics Washing. In M.D. DUBBER, F. PASQUALE, & S. DAs (Eds.), *The Oxford Handbook of Ethics of AI* (pp. 76-106). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190067397.013.5

ZALNIERIUTE, M. (2022). Big Brother Watch and Others v. the United Kingdom. *American Journal of International Law,* 116(3), 585-592. https://doi.org/10.1017/ajil.2022.35.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET