Received: 31 May 2024 | Revised: 22 October 2024 | Accepted: 8 December 2024

DOI: 10.1002/aaai.12207

ARTICLE

The role and significance of state-building as ensuring national security in the context of artificial intelligence development

Vitaliy Gumenyuk[1] | **Anatolii Nikitin**[2] | **Oleksandr Bondar**[3] | **Iaroslav Zhydovtsev**[4] | **Hanna Yermakova**[5]

[1]Department of Theory and History of the State and Law, KROK University, Kyiv, Ukraine

[2]Odesa State University of Internal Affairs, Odesa, Ukraine

[3]Department of Civil and Legal Disciplines, Educational and Scientific Institute of Law and Innovative Education, Dnipropetrovsk State University of Internal Affairs, Dnipro, Ukraine

[4]Department of Criminal Investigations of the Educational, Research Institute of Economic Security and Customs, State Tax University, Irpin, Ukraine

[5]Research Department, Taras Shevchenko National University of Kyiv, City of Kyiv, Ukraine

Correspondence
Vitaliy Gumenyuk, Department of Theory and History of the State and Law, KROK University, Kyiv, Ukraine.
Email: vitaliy_gumenyuk@sci-univ.com

Abstract

Artificial intelligence (AI) has emerged as a major technology and represents a fundamental and revolutionary innovation of our time that has the potential to significantly change the global scenario. In the context of further development of artificial intelligence, state establishment plays a central role in ensuring national security. Countries are tasked with developing legal frameworks for the development and application of AI. Additionally, governments should commit resources to AI research and development to ensure access to cutting-edge technology. As AI continues to evolve, nation-building remains crucial for the protection of national security. Countries must shoulder the responsibility of establishing legal structures to supervise the progression and implementation of artificial intelligence. Investing in AI research and development is essential to secure access to cutting-edge technology. Gracious society and open engagement apply critical impact on forming AI approaches. Civic organizations can contribute to expanding open mindfulness of the related dangers and openings of AI, guaranteeing straightforwardness and responsibility in legislative activities, and pushing for the creation of capable AI approaches. Open interest can help governments in comprehending the yearnings of citizens with respect to AI approaches. This study explores the role and importance of nation-building in ensuring national security in the context of the development of artificial intelligence. It also examines how civil society and public participation can effectively shape AI policy. The topic offers diverse research and analytical opportunities that enable a deeper understanding of the interactions and mutual influences between statehood and artificial intelligence in the context of ensuring national security. It examines the potential and threats that artificial intelligence poses to national security and considers strategies that countries can adopt to ensure security in this area. Based on the research findings, recommendations and suggestions are made for governments and civil society to improve the effectiveness of public participation in formulating AI policies.

INTRODUCTION

In the contemporary world, where the role of artificial intelligence (AI) is crucial for national security, this article examines key aspects of state-building in the context of AI development. The primary objective of the research is to analyze the role played by the state in ensuring national security through the formulation of AI policies, as well as to explore how civil society and public participation can influence this process (Kgoale and Odeku 2023).

The method of state-building within the domain of AI goes past the state's capacity to supervise innovative advance; it moreover includes making procedures that point to maximizing national security benefits (Korniienko et al. 2020). The effect of state-building on AI advancement and the need to adjust lawful and administrative systems are significant contemplations. Within the setting of AI, state-building alludes to how a state shapes its approaches, laws, and teaching to address challenges and openings related to AI.

The viable utilization of AI can be a key to calculating and upgrading the effectiveness of the national state-building framework. On one hand, the state can utilize AI to optimize capacities within the security space, such as defending basic framework, improving cybersecurity, combating psychological warfare, and securing borders. On the other hand, it is fundamental to address potential threats, just like the abuse of AI for cyber-attacks, the improvement of unused weapons, and the potential work relocation coming about from AI headways, and execute preventive measures. Within the setting of AI, respectful society plays a pivotal part in forming arrangements. Dynamic open cooperation contributes to straightforwardness and the thought of different viewpoints in creating AI methodologies. It is imperative to investigate how respectful society can offer assistance, relieve dangers, and ensure the moral use of AI. Examining various models of public participation in AI policy development allows us to identify optimal approaches to ensure effective and legitimate regulation. Successful and unsuccessful examples of public involvement define the context of effective strategies and point toward potential avenues for further improvement (Golovin et al. 2022).

State-building in the context of AI is defined not only by the state's ability to regulate and control technological development but also by the creation of strategies aimed at maximizing benefits for national security. The impact of state-building on innovative progress in AI and the necessity of adapting legal and regulatory frameworks are significantly considered. In the context of AI, state-building can be defined as the process in which the state shapes its policies, legislation, and institutions to address challenges and opportunities related to AI.

The utilization of AI can be a key factor in ensuring the efficiency of the national state-building system. On one hand, the state can use AI to optimize its functions in the security domain, such as protecting critical infrastructure, advancing cybersecurity, countering terrorism, and securing borders; on the other hand, it is essential to consider potential threats, misuse of AI for cyber-attacks, the development of new weapons, and the reduction of jobs resulting from AI development, and take preventive measures.

In the context of AI, civil society can play a crucial role in policy formation. Active public participation can contribute to transparency and consideration of diverse perspectives in the development of AI strategies. It is crucial to examine how civil society can help mitigate risks and ensure ethical use of AI. Exploring various models of public participation in AI policy development allows for identifying optimal approaches to ensure the effectiveness and legitimacy of regulation. Successful and unsuccessful examples of public participation define the context of successful strategies and indicate possible avenues for further improvement.

A detailed analysis of potential advantages and risks of AI in the context of national security provides a comprehensive framework for management and regulation. Examining measures aimed at reducing threats and maximizing benefits from AI helps create a balanced strategy. Based on research, specific recommendations are developed for the government and civil society. This includes improving mechanisms of public participation, creating a conducive environment for AI development, and defining ethical norms for technology use.

The purpose of the study is also to provide concrete examples of measures that can be taken or considered. The first is the creation of a national body on AI, which will be responsible for the development and implementation of policy in the field of AI. The second implementation of the certification system for AI systems used in critical infrastructures. The third is the creation of AI research centers and laboratories that will develop advanced AI technologies. The fourth implementation of AI educational programs in higher education institutions. This subject isn't as it were significant within the setting of the present-day world but is additionally significant for understanding and actualizing procedures that empower nations to viably tackle the benefits of counterfeit insights for their security and flexibility.

The research demonstrates the evolution of the state's role in shaping policies related to artificial intelligence, starting from the development of initial concepts and concluding with current strategies and decisions of national governments. It is essential to identify how states collaborate with the private business sector, research institutions,

and international organizations to promote the development and implementation of AI technologies with a focus on national security. The research will encompass civil society and its potential influence on shaping policies in the field of AI. Various models of civic participation and their contribution to the development of effective and ethical strategies for using AI in the interest of national security are analyzed. Special attention is given to potential threats arising from the development of artificial intelligence to national security. This includes cybersecurity issues, the potential misuse of technologies, as well as social and economic aspects such as job loss and changes in the economic structure.

Based on the obtained results, recommendations have emerged for governments and civil society on the optimal use of AI technologies, considering national security. These recommendations aim to strike a balance between fostering innovation and minimizing potential risks for society and the state. In conclusion, the research reveals a deep interconnection between state-building, AI, and national security. The implementation of our recommendations can be a step towards creating a safer and more resilient society in the era of rapid technological development.

LITERATURE REVIEW

The integration of AI into state-building processes, especially with regard to national security, presents unique challenges and opportunities. As AI technologies continue to evolve, so does their potential to strengthen or undermine the structures that keep the state safe. This literature review summarizes research on cybersecurity, AI reliability, and the responsible deployment of AI, offering insights into how it can be integrated effectively into state-building processes to ensure national security.

In the context of nation-building and national security, cybersecurity has become a critical issue. For example, deepfakes are a growing threat to state stability because of their potential to disrupt public trust and democratic processes. According to Kumar et al. (2024), strategies to mitigate the spread of disinformation through deepfakes are important to protect national security. These strategies include AI-driven detection algorithms that promote digital literacy among citizens. The researcher notes that without reliable countermeasures, the development of deepfake technology can destabilize political institutions, manipulate public opinion, and weaken the state security system.

The shift to decentralized financial systems also complicates cybersecurity efforts. Sahu and Kumar (2024) discuss how blockchain and other decentralized technologies can strengthen the state's financial infrastructure, making it less vulnerable to centralized attacks. Thus, decentralized finance offers a secure alternative that can protect national financial systems from cyberattacks. However, they highlight the need for proper management structures to manage these systems and ensure their security.

The role of AI in state-building largely depends on the reliability of technologies. Predicting and mitigating software vulnerabilities is critical in this context. Sahu and Srivastava (2021) emphasize the importance of reliable software to maintain state security. This approach permits the anticipation of errors and vulnerabilities in critical software systems, ensuring that the technology supporting the national infrastructure remains safe. Similarly, Kumar, Ahmad Khan, and Ahmad Khan (2023) explore how durable software can be developed and maintained over time, especially in environments that are critical to state building, such as defense, infrastructure, and public administration. Robust software ensures that AI systems remain functional and resilient to new threats, thereby contributing to national security.

The application of AI in the security of military computing environments is another important research area. Thus, Kumar and Khan Raees (2024a, 2024b) emphasize the role of AI and blockchain technologies in strengthening military infrastructures. They describe how AI-driven security protocols can protect sensitive communication channels from cyber-attacks, during military operations. For instance, blockchain offers improved data integrity and transparency, ensuring that military data and communications are protected from external threats.

Furthermore, Pandey et al. (2024) discuss how AI can be applied to protect the healthcare system, which is also targeted by cyberattacks. Integrating AI into smart health systems enables real-time threat detection and response, which is critical to maintaining state resilience against cyber-attacks on public infrastructure.

Another pressing challenge in using AI to ensure national security is the ethical and responsible use of technologies. In this regard, Radanliev et al. (2024) analyze the ethical dilemmas that AI creates in military and state security programs. They advocate the development of transparent AI systems that give priority to human rights and the rule of law. This is especially important for state-building in order to avoid abuse and violations of civil liberties. Similarly, Radanliev (2024) explores the importance of incorporating ethical considerations into the development of AI systems from the outset. The researcher argues that AI systems used in state security should be safe, reliable, and transparent to ensure that they do not accidentally harm the citizens they are supposed to protect. The ethical usage of AI involves the creation of a framework that prevents its misuse by state and non-state institutions.

The reviewed literature emphasizes the transformational potential of AI in strengthening state-building, especially in the field of national security. However, it also highlights the need for robust cybersecurity measures, secure AI systems, and ethical use. As AI continues to evolve, states must adopt comprehensive strategies to address the technical, ethical, and security challenges associated with this technology. By integrating AI responsibly and safely, states can increase their resilience to traditional and emerging threats.

METHODOLOGICAL FRAMEWORK

The study focused on employing various approaches for investigation. Specifically, the systemic approach allowed for the examination of state-building within the context of AI development as an intricate system involving the interactions among the state, civil society, and AI. The historical approach delved into the evolution of this process, while the comparative approach facilitated the comparison of experiences across different countries in this field.

To conduct the research, diverse methods and tools were utilized, such as document analysis (including normative-legal documents, strategies, and programs), expert interviews, and observation of the policy formation process in the AI sector. The findings emphasized that state-building in the context of AI development is a multifaceted process, entailing the dynamic interplay among the state, civil society, and AI. AI can function both as a tool for national security and as a potential source of threats. The pivotal role of civil society in influencing policies in this domain was underscored (Kovalova, Korniienko, and Postol 2019).

Drawing from the research results, recommendations were formulated for both the government and civil society. These recommendations encompass enhancements to mechanisms facilitating public participation in shaping AI policies, the creation of an enabling environment for AI development in countries affiliated with the United Nations and NATO, and the establishment of ethical norms governing the use of AI.

The research reveals a deep connection between state-building, AI, and national security. Implementing the recommendations can contribute to the creation of a safe and resilient society amidst rapid technological development. Although the research has numerous advantages, such as a broad spectrum of issues and in-depth material analysis, it also has limitations: static nature, failure to consider the dynamics of AI and national security development, and a focus on specific countries that restricts the applicability of conclusions to other nations.

For a better understanding of the interplay between state-building, AI, and national security, it is recommended to conduct research on the dynamics of AI development, comparative analysis of different countries' experiences in state-building in the context of AI development, and modeling various scenarios of AI development and their impact on national security. Considering the global nature of AI and its influence on international security is crucial. The research is expanded to examine aspects of cybersecurity, especially in the context of AI utilization in government and defense. Additional analyses of risks and security measures can aid in developing effective strategies to prevent potential threats.

All these research directions will help broaden the understanding of the interconnection between AI development, state-building, and national security, contributing to the creation of comprehensive and adaptive strategies for different countries in the rapidly changing technological environment.

RESULTS AND DISCUSSION

In the modern information society, the role of AI has become increasingly significant, especially in the context of national security. AI plays a key role in addressing challenges related to cybersecurity, protecting critical infrastructure, and other aspects of national security. Understanding and analyzing the interaction between the state, civil society, and artificial intelligence becomes crucial for effectively ensuring the security and resilience of national systems (Smokov et al. 2022).

The investigative subject centers on investigating the part and noteworthiness of state-building within the setting of counterfeit insights advancement and its effect on national security. This subject stands out due to the significance of understanding and optimizing the interaction between government structures and the advancement of AI innovations to maximize the productivity of the country's security framework. It is most important within the course of the inquiry to address how the state can adjust its political, legitimate, and administrative instruments to lock in with the improvement of fake insights and how this interaction impacts the national security framework. Inside this think about, the part of gracious society and open participation in forming AI approaches and their impact on guaranteeing national security is additionally examined (Boyko et al. 2020).

In the context of national security and artificial intelligence, it is crucial to examine the role and interest of NATO in these matters. NATO, as a military-political alliance, is tasked with ensuring the security of its members and defending against threats from external actors (Suray et al. 2019). NATO recognizes the significance of AI advancement to improve its resistance techniques. Inside

the system of a key association with the AI segment, the organization together investigates openings to utilize imaginative advances for making strides in insights, cybersecurity, and other viewpoints of security. NATO recognizes that AI improvement has the potential to altogether improve the alliance's protection capabilities. AI can be utilized to move forward insights, cybersecurity, troop administration, and other security angles. In any case, the advancement of AI is additionally related to certain lawful challenges (Stanley-Lockman and Christie 2021).

One of the essential legal challenges is the need to create modern lawful systems to control the advancement and use of AI. Current legitimate systems, such as worldwide law and national enactment, frequently do not account for the particular characteristics of AI. For this case, worldwide law needs particular standards directing the utilization of AI for military purposes. NATO is effectively working on creating unused legitimate systems for AI. In 2023, the union embraced the "NATO Vital Concept on Counterfeit Insights," sketching out key standards and approaches for the improvement and utilization of AI inside the organization together. The concept envisions NATO collaborating with other nations and universal organizations to create worldwide legitimate systems for AI (Kornieieva 2021).

Another legal challenge is the need to protect human rights and fundamental freedoms when using AI. AI can be employed to create new technologies that may have a negative impact on human rights, such as developing AI systems capable of making life-and-death decisions for individuals. NATO recognizes the importance of safeguarding human rights and fundamental freedoms in the use of AI. In the "NATO Strategic Concept on Artificial Intelligence," the Alliance declared its commitment to using AI "in a manner consistent with international law, NATO principles, and values, such as the rule of law, democracy, and human rights" (Summary of the NATO Artificial Intelligence Strategy 2021). NATO is also actively working on developing ethical norms for AI usage. In 2022, the Alliance adopted the "NATO Ethical Principles on Artificial Intelligence," establishing fundamental principles to guide NATO countries in using AI. These principles include:

- AI should be used in a manner consistent with international law, NATO principles, and values, such as the rule of law, democracy, and human rights.
- AI should be used in a transparent and accountable manner.
- AI should be used in a manner that is safe and reliable.

The development of new legal frameworks and ethical norms for AI is a crucial task for NATO. These measures will help the Alliance ensure that AI is used in a manner consistent with its values and contributes to the security of Europe and North America. The development of AI systems capable of making life-and-death decisions for individuals, such as managing military systems like drones, raises concerns about their reliability and potential for discrimination (Malii 2021). One key area of interaction is cybersecurity, as AI plays a significant role in this dimension. NATO focuses on improving cybersecurity and exploring the possibilities of using artificial intelligence to counter cyber threats. The use of AI to create cyber weapons is another consideration. Cyber weapons are software designed to harm computer systems or networks. AI can be used to develop more effective and dangerous cyber weapons.

The use of AI for mass surveillance systems is also a concern. AI can analyze large volumes of data, such as internet data or video feeds, potentially leading to violations of citizens' privacy. NATO recognizes the importance of considering not only military but also civilian and societal aspects of AI. The Alliance is fostering partnerships with civil society and the private sector to exchange knowledge, develop ethical standards, and collaboratively devise strategies for the use of artificial intelligence. Considering NATO's contribution to the global discourse on the use of artificial intelligence in the defense sector, we expand our research by incorporating aspects of international cooperation and the exchange of best practices among alliance member countries (Hunter et al. 2018).

State-building is an ongoing process involving the creation and development of an effective governing body capable of ensuring national security. National security encompasses the state of safeguarding a nation's vital interests from potential threats, both internal and external. In the context of AI, the state-building process involves establishing efficient institutions and strategies that enable a country to regulate the development and utilization of AI effectively (Karmaza and Kusherets 2021). The key tasks of these institutions and strategies include:

- The state must be capable of confronting potential threats to national security associated with the application of AI.
- The use of AI should not lead to violations of fundamental rights and freedoms of individuals.
- AI can be beneficial for improving the quality of life and economic development.

The state should formulate legal standards that define the conditions for the development and use of AI, taking into account the interests of both the state and society. Collaboration between states and international organizations is essential for determining and implementing common legal standards and ethical norms for AI. This is

crucial to ensuring the coherence of legislative norms and preventing the misuse of AI in hybrid warfare and other forms of aggression.

The United Nations and countries are working together to ensure national security in terms of AI development. The United Nations has developed international legal frameworks and ethical standards for AI, and countries are integrating these frameworks into their national laws and policies. This interaction is important to ensure that AI is used in a manner that complies with international law and promotes peace and security around the world. The United Nations recognizes that advances in AI have the potential to significantly improve international peace and security. AI can be used to improve intelligence, cybersecurity, conflict prevention, and other security aspects. However, the development of AI also comes with challenges, including the fact that international and domestic laws often do not fully take into account the special features of AI. Addressing the need to protect human rights and fundamental freedoms in the use of AI, which can be employed to create new technologies with potential negative impacts on human rights, such as AI systems capable of making decisions about life and death, is crucial.

The United Nations plays an important role in ensuring national security in terms of AI development. The United Nations is working to develop a new legal and ethical framework for AI to ensure that AI is used in a manner consistent with international law and to promote global peace and security. United Nations action to ensure national security related to the development of AI. The United Nations is working to develop international legal standards governing the development and use of AI. These norms must take into account the interests of all countries in the world, both developed and developing countries. The United Nations is working to develop international legal norms that protect human rights and fundamental freedoms when using AI. These rules should ensure that AI is not used to discriminate or violate human rights. The United Nations is working with other countries and international organizations to develop and implement legal frameworks and ethical standards regarding AI. This cooperation is essential to ensure that AI is used in a manner that complies with international law and promotes global peace and security (Madi and Al Shamsi 2023).

A certain state that is interested in AI should develop and improve legal norms that regulate the development and use of AI. This includes legislation that defines ethical standards, rules for the use of military aspects of AI, and also defines responsibility for violations of these norms. States should also fund AI research and development to ensure access to advanced technologies and maintain national competitiveness. The successful implementation of AI requires an appropriate infrastructure, which includes powerful computing resources, large volumes of data, and fast communication networks. The state should promote the creation of such infrastructure. It is possible that the laws may even provide security standards for AI systems used in critical infrastructures, as well as prohibit the development and use of autonomous weapons systems. For the effective use of AI, the state should invest in the education and training of specialists in the field of artificial intelligence. This may include the development of training programs, internships, and research support.

To protect against potential cyber threats, the state should improve cyber security systems and implement measures to avoid unauthorized access to AI technologies, as well as to create a legal framework that regulates the development and use of AI. These frameworks should aim to ensure safety, ethics, and transparency in the field of AI.

No less important is the very interaction of state-building and AI. I will repeat repeatedly that the development of AI has a wide range of opportunities for state building. AI can be used to improve the efficiency of public administration, strengthen national security, and ensure economic growth. The state should actively promote the development and establishment of ethical standards for the use of AI. This may include determining the limits of using personal information, protecting human rights, and other ethical aspects. However, the development of AI is also associated with a number of issues and problems for state-building. These challenges become more important to discuss with each new step of AI. States must take steps to address the challenges to ensure that AI is used to advance national interests and security. The state should establish monitoring and regulatory systems in the field of AI to ensure compliance with legal norms and ethical standards. This approach allows the state to effectively interact with AI, maximizing its positive impact on national security.

Involvement of civil society in the formation of policy in the field of AI allows for ensuring transparency and consideration of different points of view. Public participation can serve as a tool to reduce risks and increase citizens' trust in the use of AI. Civil society is considered a collection of non-governmental organizations and groups, such as non-profit organizations, public organizations, trade unions, religious organizations, and citizen activists, and plays an important role in modern democratic societies. Its tasks include ensuring transparency, monitoring government measures, and protecting the interests of different social groups. We would like to remind you that the aim and objective of this article is to consider the opportunities and challenges of civil society interaction with AI systems and the implications for ethical issues. Civil society faces ethical issues related to the use of AI, including discrimination, data protection violations, and liability for the behavior of AI systems.

It is essential to develop an ethical framework for using these technologies. Civil society can play an important role in raising awareness of these issues and contributing to the development of ethical standards. Civil Society Initiative, there is an opportunity for civil society to actively influence the shaping of AI policy through various instruments such as conducting research, organizing public discussions, engaging government representatives in dialogue, and creating lobbying groups. Their involvement in shaping AI policy can lead to increased public awareness of the risks and opportunities of these technologies, ensure transparency in government actions, and contribute to the development of responsible AI policies. Civil society can actively contribute to the development of ethical standards and identify areas where the use of AI should be restricted or regulated.

This may include developing codes of conduct for AI developers and users and enforcing laws governing the use of AI in areas such as discrimination and data breaches. Public authorities can participate in expert groups, consultations, and other forums to actively influence the design of AI policy. A key aspect of this process is involving the community in developing the AI strategy and development plan. In recent years, AI has been able to transform national security strategies, presenting significant opportunities but also serious challenges. On the positive side, the introduction of AI will improve the efficiency of information processing and enable critical national security missions to be addressed. Automated systems can analyze large amounts of data and respond to potential threats in real time. AI-based predictive models can help prevent and detect threats, significantly increasing predictive accuracy.

However, there are serious risks associated with the use of AI in the context of national security. Cyber threats and the potential for AI abuse require special attention. Adversaries may use these technologies for targeted attacks, threatening both security and the confidentiality of crucial data. Concurrently, issues of confidentiality and privacy are also important to consider. Mass data collection and processing can violate citizens' basic privacy rights, requiring careful attention to ethical standards and regulations.

Avoiding technological dependence and addressing ethical issues when using AI are also important challenges for national and international organizations. It is important to ensure that the introduction of AI into national security systems not only increases efficiency but is also ethical and consistent with the principles of the rule of law. More generally, discussing the benefits and risks of using AI for national security in an international context is an important step toward understanding and addressing these complex issues. The development of international standards and common strategies can contribute to the optimal use of AI to support security and stability around the world. In the previous paragraphs, where risks in AI were discussed to ensure security at the state level, measures and maximum benefits for advanced AI technologies were proposed. International organizations such as NATO and the UN, along with progressive countries, are considering measures aimed at ensuring security in the field of AI that can be implemented by states. These measures involve the need to develop and implement international standards to ensure the ethical use of AI. This will help prevent unauthorized use of the technology and ensure a responsible approach.

The introduction of certification systems for AI guarantees compliance with safety and ethics standards. This will increase trust in AI systems and ensure their security. Training programs and awareness initiatives are important for shaping an informed approach to AI among professionals and citizens. The creation of independent mechanisms to control the use of AI will help identify and regulate potential shortcomings. Participation in international initiatives to jointly address ethical, legal, and security issues in AI is crucial for the successful implementation of the technology.

The requirement for AI developers to publish algorithms contributes to their transparency and societal trust. The development of specialized centers for detecting and countering cyber threats in the field of AI is critically important for ensuring security. Table 1 shows the key aspects of AI use in terms of state-building and national security.

The implementation of these measures requires joint efforts from governments, the public, and international organizations. Only a comprehensive approach to ensuring security in the field of AI can ensure the stable and ethical development of this promising technology as it advances in its developmental journey.

The rapid development of AI technologies created unprecedented opportunities and challenges for national security. While the AI potential to enhance state-building and strengthen security measures is clear, its unregulated use could pose risks to national sovereignty, civil liberties, and international stability.

AI technologies are developing rapidly, but the legal frameworks governing their use in national security remain outdated or absent. To ensure responsible implementation, governments must prioritize the creation of a comprehensive legal framework that can tackle the AI-related challenges and define the permitted use of AI in national security. This framework should uphold human rights, data protection, and AI accountability. In addition, countries should cooperate to create a coherent policy on the use of AI to avoid misuse or global insecurity.

The limits of AI use in the context of national requires clear ethical boundaries. Otherwise, AI can be used to

TABLE 1 Key aspects of AI usage for state-building and national security.

Sphere	Key aspects
Role of AI in national security	AI's significant role in cybersecurity and protecting critical infrastructure - Interaction between state, civil society, and AI is crucial for national security
State-building and AI development	- Optimizing government structures for AI development - Adjusting political, legal, and regulatory tools to enhance national security using AI
NATO's AI strategy	- AI is essential for enhancing defense capabilities - "NATO Strategic Concept on AI" outlines legal frameworks and collaboration with other nations to regulate AI
Legal and ethical challenges	- Need for new legal frameworks for AI regulation - Ensuring AI systems comply with human rights, rule of law, and democracy principles - "NATO Ethical Principles on AI" promote transparency and reliability
Cybersecurity and AI	- AI's role in developing cyber weapons and improving cybersecurity - Mass surveillance concerns involving AI and potential privacy violations
International cooperation	- UN's role in developing legal and ethical AI standards - Collaborating with international organizations for AI regulation to promote peace and security globally
State's role in AI regulation	- Legal standards for AI development and use - Investments in AI research, infrastructure, and human resource development for national competitiveness
Civil society's involvement	- Civil society ensures transparency and influences AI policy - Public participation helps raise awareness of AI's risks and benefits, influencing ethical standards
AI in public administration	- AI improves public governance, strengthens national security, and promotes economic growth - Ethical standards and regulation are crucial for AI's development in state-building
Ethical AI use	- Developing global ethical standards for AI is critical - The need for certification systems, training programs, and independent control mechanisms to ensure AI's safe and ethical application
Global risks and opportunities of AI	- AI enhances information processing for national security missions - Risks include cyber threats, AI abuse, mass surveillance, and technological dependency
Measures to ensure AI security	- International collaboration for ethical AI use - Certification and transparency of AI algorithms to ensure compliance with safety and ethical standards

undermine civil liberties or violate international law. Establishing clear ethical principles for the use of AI should regulate areas such as surveillance, autonomous decision-making in warfare, and data privacy. They should be mandatory to ensure continued compliance with the standards of human rights protection.

Furthermore, AI technologies in critical national security sectors are vulnerable to cyber-attacks. Using AI as weapons poses a serious threat, requiring the protection of AI systems from external interference. Accordingly, critical sectors of government agencies, defense sectors, and cybersecurity companies should collaborate to build resilient AI systems that are difficult for cybercriminals or foreign states to hack.

Moreover, given the global nature of AI technologies, countries should cooperate in developing international norms and standards for the use of AI in national security. International organizations such as NATO and the UN should lead the effort to establish global agreements on AI in the defense sector. Such a cooperation would prevent the spread of uncontrolled AI technologies that can provoke global conflicts.

The AI application in national security often raises public concerns about privacy and civil liberties. Transparency and engagement with civil society are crucial to mitigate these problems and enhance public trust. Governments should involve NGOs, human rights organizations and the public in the policy-making process. To ensure accountability in the use of AI for national security, independent oversight bodies should also be created. These organizations would oversee AI use and enforce international legal and ethical standards.

Governments and businesses should create and fund specialized training programs in AI technology and cybersecurity for national security experts. Moreover, a group of experts on the use of AI for defense purposes should be created on the basis of universities and business. In this connection, investments in education will promote the state's competitiveness in the global race of AI while adhering to ethical standards.

Therefore, the AI integration into national security poses risks. However, by applying urgent coordinated measures, industries can adapt to new challenges. By prioritizing the development of robust legislative frameworks, ethical standards, and cybersecurity measures while promoting international cooperation and public transparency, the security sector can harness AI responsibly and safely. These efforts will protect national

interests and the fundamental rights of citizens in the era of AI.

CONCLUSION

National security emerges as a paramount concern amid the rapid evolution of AI, demanding the attention of statesmen to delineate effective strategies and policies. In the exploration of this subject, specific inquiries have been posited, and analyses conducted to unveil pivotal facets of the role of statecraft and the significance of national security in the context of AI development.

In the swiftly advancing landscape of AI, national security assumes novel dimensions. Critical considerations include the identification and safeguarding of essential infrastructures, cybersecurity, as well as the regulation of ethical and legal aspects concerning AI usage. Statesmen must actively engage in the development and implementation of cybersecurity strategies, the creation of robust legislative frameworks, and the promotion of innovations in the security domain to eliminate potential threats.

The ability of nations to collaborate and establish international standards in the realm of cybersecurity becomes imperative. Strengthening global partnerships and exchanging best practices can contribute to effectively countering threats. The ethical use of AI in military affairs necessitates the formulation of international norms and standards that restrict the potential misuse of AI for aggressive purposes. Nations should actively facilitate the development and implementation of ethical norms and legislative constraints to avert potential adverse consequences of AI usage and prevent threats.

In conclusion, statesmen must define national strategies that account for the impact of AI on national security and actively collaborate internationally to create effective international mechanisms for control and regulation. Safeguarding national security in the era of AI development requires a comprehensive approach and global cooperation.

ACKNOWLEDGMENTS

The authors did not receive support from any organization for the submitted work. No funding was received to assist with the preparation of this manuscript. No funding was received for conducting this study. No funds, grants, or other support was received.

CONFLICT OF INTEREST STATEMENT

The authors declare that there is no conflict.

ETHICS STATEMENT

All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

CONSENT TO PARTICIPATE

Informed consent was obtained from all individual participants included in the study.

CONSENT FOR PUBLICATION

All individual participants agreed to be included in the study.

ORCID

Vitaliy Gumenyuk https://orcid.org/0009-0004-0654-8066

REFERENCES

Boyko, A., G. Vlasova, S. Omelyanchyk, O. Bondar, D. Moroz, and R. Karpenko. 2020. "Political and Legal Aspects of Regulating Transnational Labour Migration." *International Journal of Advanced Research in Engineering and Technology* 11(5): 153–63.

Golovin, D., Y. Nazymko, O. Koropatov, and M. Korniienko. 2022. "Electronic Evidence in Proving Crimes of Drugs and Psychotropic Substances Turnover." *Access to Justice in Eastern Europe* 5(2): 156–66.

Hunter, A. P., L. R. Sheppard, R. Karlenand, and L. Balieiro. 2018. *Artificial Intelligence and National Security: The Importance of the AI Ecosystem*. Washington: Center for Strategic and International Studies.

Karmaza, O. O., and D. V. Kusherets. 2021. Artificial Intelligence in the Civil Process: Prospects for Use. http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/102/2586/5540-1?inline=1

Kgoale, T. J., and K. O. Odeku. 2023. "An Analysis of the International and European Union Legal Instruments for Holding Artificial Intelligence Accountable." *Juridical Tribune* 13(3): 427–40.

Kornieieva, S. 2021. "Normative and Legal Bases of Regulation of Artificial Intelligence in Foreign Countries and Ukraine." *Visegrad Journal on Human Rights* 21: 4105–111.

Korniienko, M. V., I. V. Petrunenko, I. V. Yena, K. O. Pankratova, and K. A. Vozniakovska. 2020. "Negative Effects of Corruption Offenses for the Country's Economy." *International Journal of Management* 11(5): 1072–83.

Kovalova, O., M. Korniienko, and O. Postol. 2019. "Ensuring of Child's Dignity as a Principle of Modern Education: Administrative and Legal Aspects." *Asian International Journal of Life Sciences* 21(2): 341–59.

Kumar, R., and A. Khan Raees. 2024a. "Securing Communication Protocols in Military Computing." *Network Security* 2024(3). https://www.magonlinelibrary.com/doi/abs/10.12968/S1353-4858%2824%2970011-7.

Kumar, R., and A. Khan Raees. 2024b. "Securing Military Computing with the Blockchain." *Computer Fraud & Security* 2024(2). https://doi.org/10.12968/S1361-3723(24)70007-4.

Kumar, R., S. Ahmad Khan, and R. Ahmad Khan. 2023. *Software Durability: Concepts and Practices* (1st ed.). Boca Raton, FL: CRC Press. https://doi.org/10.1201/9781003322351.

Kumar, R., S. Ahmad Khan, N. Alharbe, and R. Ahmad Khan. 2024. "Code of Silence: Cyber Security Strategies for Combating

Deepfake Disinformation." *Computer Fraud & Security* 2024(4): 1361–3723. https://doi.org/10.12968/S1361-3723(24)70013-X.

Madi, R., and I. Al Shamsi. 2023. "Granting Inventor Status to AI in Biotechnology Patents: A Regional Perspective of the Patent Laws in the Gulf Cooperation Council Countries." *Industrial Biotechnology* 19(5): 272–80.

Malii, M. 2021. "Prevention of Computer Crimes electronic Intelligence Against Human, Society, State." *Visegrad Journal on Human Rights* 4: 143–51.

Pandey, A. K., A. K. Das, R. Kumar, and J.J.P.C. Rodrigues. 2024. "Secure Cyber Engineering for IoT-Enabled Smart Healthcare System." *IEEE Internet of Things Magazine* 7(2): 70–77. https://doi.org/10.1109/IOTM.001.2300172.

Radanliev, P. 2024. "Digital Security by Design." *Security Journal* 37: 1640–79. https://link.springer.com/article/10.1057/s41284-024-00435-3#citeas

Radanliev, P., O. Santos, A. Brandon-Jones, and A. Joinson. 2024. "Ethics and Responsible AI Deployment." *Frontiers in Artificial Intelligence* 7: 1377011. https://doi.org/10.3389/frai.2024.1377011.

Sahu, K., and R. Kumar. 2024. "A Secure Decentralised Finance Framework." *Computer Fraud & Security* 2024(3): 1361–3723. https://doi.org/10.12968/S1361-3723(24)70010-4.

Sahu, K., and R. K. Srivastava. 2021. "Predicting Software Bugs of Newly and Large Datasets Through a Unified Neuro-Fuzzy Approach: Reliability Perspective." *Advances in Mathematics: Scientific Journal* 10(1): 543–55.

Smokov, S. M., V. V. Horoshko, M. V. Korniienko, and S.V. Medvedenko. 2022. "Rule of Law as a Principle of Criminal Procedure (on Materials of the European Court of Human Rights)." *Pakistan Journal of Criminology* 14(3): 37–46.

Stanley-Lockman, Z., and E. H. Christie. 2021. "Artificial Intelligence Strategy for NATO." *NATO Review*, October 25, 2021. https://www.nato.int/docu/review/uk/articles/2021/10/25/strategya-shchodo-shtuchnogo-rozumu-dlya-nato/index.html.

Summary of the NATO Artificial Intelligence Strategy. 2021. NATO, October 22, 2021. https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

Suray, I., S. Suprunenko, O. Kartashova, O. Bondar, V. Gerashcenko, and R. Karpenko. 2019. "Public Administration and Innovation Policy in a Networked Society." *International Journal of Recent Technology and Engineering* 8(4): 3604–9.

How to cite this article: Gumenyuk, V., A. Nikitin, O. Bondar, I. Zhydovtsev, and H. Yermakova. 2025. "The role and significance of state-building as ensuring national security in the context of artificial intelligence development." *AI Magazine* 46: e12207. https://doi.org/10.1002/aaai.12207

AUTHOR BIOGRAPHIES

Vitaliy Gumenyuk: PhD legal sciences, associate professor of the Department of Theory and History of the State and Law, KROK University. I actively engage in scientific research and have authored numerous publications in the fields of criminal law, theory and history of state and law, and electoral law. I have extensive teaching experience in legal disciplines, mentoring young researchers, and participating in academic conferences. Professional Interests: Criminal Law and Procedure, Electoral Law and Administrative Process, History and Theory of State and Law, Current Issues of Legal Policy in Ukraine.

Anatolii Nikitin: Vice-Rector of the Odesa State University of Internal Affairs, Candidate of Legal Sciences (PhD in law), associate professor, and police colonel. Professional Interests: Criminal Law and Criminology, Public Safety and Law Enforcement Management, Legal Regulation of Temporarily Occupied Territories, Higher Education in Law Enforcement.

Oleksandr Bondar: PhD in law, associate professor, Department of Civil Law Disciplines, Dnipropetrovsk State University of Internal Affairs. Author of 57 publications, including 52 scientific papers and 5 educational and methodological works. Published research in national and international peer-reviewed journals, with two articles indexed in Scopus and Web of Science. Scientific Interests: Labor Law and Social Security Law, Civil Law and Legal Regulation of Employment Relations, Comparative Legal Analysis of Social Protection Systems.

Iaroslav Zhydovtsev: PhD in law, associate professor at the Department of Criminal Justice and Analytical Activities, Educational and Scientific Institute of Economic Security and Customs Affairs, State Tax University. Author of 15 scientific papers in the fields of criminal procedure, forensics, and operational-investigative activities. Professional Interests: Operational and investigative activities, criminal procedure and forensic expertise, traffic accident investigations, information protection and analytics, public safety, and crime prevention.

Hanna Yermakova: PhD in law, associate professor of the Research Department, Taras Shevchenko National University of Kyiv. Doctoral Researcher, Institute of Legislation, Verkhovna Rada of Ukraine. Candidate of Philosophical Sciences (PhD) in Religious Studies, Taras Shevchenko National University of Kyiv. Professional Interests: Constitutional and Municipal Law, Religious Studies and Philosophy, Education Administration.