DOI https://doi.org/10.36059/978-966-397-570-2-96

Tsymbal A. S.,
Master
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
Kyiv, Ukraine

SHADOW AI AS A CYBERSECURITY AND PRIVACY CHALLENGE IN POST-WAR UKRAINE

Introduction. The rapid integration of artificial intelligence (AI) into state and corporate systems has redefined the technological landscape of modern Ukraine. As the country rebuilds its digital infrastructure after years of war, AI tools have become key drivers of modernization and efficiency across sectors such as defense, healthcare, public administration, and finance. However, this accelerated adoption has also introduced a new and often overlooked threat – Shadow AI.

Shadow AI refers to the unauthorized, non-certified, or unmonitored use of AI models within organizations or governmental structures without official oversight or compliance with cybersecurity standards. Such systems may operate outside formal data protection frameworks, process confidential information without consent, and even transmit data to third-party servers. According to Balogun et al. [1], these risks are particularly critical in sensitive fields like healthcare and finance, where data integrity and privacy are essential.

In post-war Ukraine, the implications of Shadow AI extend beyond individual organizations. The widespread deployment of unregulated AI could undermine national cybersecurity efforts, enabling potential data exploitation by foreign actors or internal vulnerabilities. As Vdovichena et al. [2] note, Ukraine's rapid digital reconstruction must be accompanied by strict governance of emerging technologies to prevent the uncontrolled diffusion of AI. Thus, addressing Shadow AI is not only a matter of technological oversight but also a fundamental component of the nation's digital sovereignty and post-war resilience.

Nature and Definition of Shadow AI. The concept of Shadow AI describes the unauthorized or uncontrolled use of artificial intelligence models within organizations or institutions. It emerges when individuals or departments employ AI systems – such as generative models or analytical tools—without official approval or compliance with cybersecurity standards. These unmonitored implementations often operate outside existing data governance frameworks, posing significant risks to data integrity, privacy, and accountability. Balogun et al. [1] emphasize that unregulated AI

adoption is especially dangerous in sectors such as healthcare, finance, and education, where even minor breaches can have ethical and legal implications.

Unlike certified AI solutions that undergo rigorous auditing and validation, Shadow AI systems often rely on open-source or third-party APIs, which may process sensitive data or transmit it to external servers without encryption. In a post-war environment where Ukraine is rebuilding its digital infrastructure, the presence of such unverified AI solutions undermines institutional resilience and erodes trust in government and corporate systems.

Cybersecurity and Privacy Risks. The primary threat of Shadow AI lies in its invisibility. Unregistered models may process confidential information, including personal identifiers, health records, or classified communications, without any traceability. Tiwo et al. [3] note that unregulated AI tools used in telemedicine have already demonstrated vulnerabilities, allowing attackers to exploit weak authentication protocols and intercept sensitive data. In the Ukrainian context, where critical systems are being rapidly digitized, such weaknesses can lead to large-scale breaches that endanger not only individuals but also state security.

Lysenko [4] highlights that AI technologies, while capable of detecting cyber threats, can paradoxically serve as instruments of attack when deployed without oversight. Shadow AI can be manipulated to generate deceptive outputs, automate phishing attempts, or bypass firewalls by mimicking legitimate traffic patterns. The post-war expansion of e-governance and digital public services further amplifies this risk, as every new system becomes a potential target for exploitation.

Moreover, the uncontrolled integration of AI into public and private databases may result in the accumulation of "invisible" datasets – information repositories created by unregistered models that store user inputs, logs, or contextual metadata. These shadow datasets are especially difficult to monitor and can be used for malicious purposes long after their creation.

Post-war Ukrainian Context. Ukraine's post-war reconstruction has become a catalyst for unprecedented digital acceleration. Artificial intelligence plays a key role in rebuilding infrastructure, improving public administration, and enhancing national defense systems. However, the rapid deployment of AI technologies without standardized regulatory mechanisms introduces systemic vulnerabilities. As Vdovichena et al. [2] argue, AI-driven initiatives in Ukraine's post-war economy have enormous potential but must be balanced with robust cybersecurity measures.

The challenge lies in the disparity between technological innovation and regulatory adaptation. Many organizations – both governmental and private – adopt AI tools independently, without coordination or alignment with national security policies. These fragmented efforts increase the likelihood of Shadow AI infiltration. For instance, an employee might use an open chatbot to draft internal reports, inadvertently exposing

classified information. Similarly, contractors working on digital reconstruction projects might deploy analytical models trained on unverified datasets, creating new avenues for cyberespionage.

In addition, the influx of foreign technologies and external funding for reconstruction amplifies dependency on imported AI solutions. Without proper localization, data processed by such systems may cross national borders, violating Ukraine's data sovereignty principles. This issue reinforces the need for a domestic framework that governs AI implementation, certification, and usage transparency.

Ethical and Legal Dimensions. The problem of Shadow AI is not limited to technical vulnerabilities – it also raises complex ethical and legal questions. Balogun et al. [1] point out that unauthorized AI applications blur the boundaries of responsibility: when a shadow model causes harm, it is often unclear who is accountable – the user, the developer, or the organization. The absence of clear accountability mechanisms leads to a regulatory vacuum, allowing unethical practices to persist.

Chaban [5] observes that Ukraine's current approach to AI regulation is still in its formative stage and must evolve to align with European Union frameworks such as the AI Act. The integration of ethical standards – transparency, fairness, and explainability – is essential to ensure public trust in AI technologies. Without such principles, Shadow AI systems will continue to proliferate, operating beyond legal boundaries and undermining democratic control over digital infrastructures.

Ethical risks also include bias, discrimination, and manipulation. In a post-conflict society like Ukraine's, where social cohesion and trust are fragile, algorithmic opacity may deepen inequalities or be weaponized for political misinformation. Therefore, developing an ethical AI governance model that prioritizes human oversight and transparency is a cornerstone of national cybersecurity strategy.

Recommendations and Future Outlook. To mitigate the threats posed by Shadow AI, Ukraine should adopt a multi-layered strategy that combines legal, technical, and educational measures. Legally, a national policy framework must define the boundaries between authorized and unauthorized AI use. Chaban [5] advocates for the establishment of a state certification body responsible for auditing and approving AI systems used in critical sectors. Technically, institutions should implement AI usage monitoring tools capable of detecting unregistered models and tracking data flows in real time.

Awareness and education are equally important. As Tiwo et al. [3] and Balogun et al. [1] suggest, training employees to understand data privacy principles and recognize potential risks can significantly reduce instances of Shadow AI emergence. Furthermore, Ukraine should promote the creation of a national register of certified AI tools, which would serve as a trusted source for developers and organizations.

In the long term, Ukraine's digital sovereignty will depend on balancing openness to innovation with strict regulatory control. The integration of ethical, legal, and cybersecurity frameworks will ensure that AI supports post-war reconstruction rather than undermines it. Shadow AI must therefore be recognized not merely as a technological anomaly but as a strategic challenge that demands continuous monitoring, policy development, and cross-sector collaboration.

Conclusions. Shadow AI represents a critical and multifaceted challenge for Ukraine's cybersecurity and privacy landscape. In the post-war context, where digital recovery and institutional modernization are top priorities, uncontrolled use of AI systems can compromise sensitive data, weaken trust in digital services, and create new vectors for cyberattacks. As Tiwo et al. [3] and Lysenko [4] emphasize, the combination of human error and insufficient regulation significantly increases these risks.

To mitigate them, Ukraine must adopt a comprehensive framework that integrates legal, technical, and educational approaches. This includes establishing clear AI certification standards, enforcing accountability mechanisms, and introducing continuous monitoring to detect unauthorized AI systems. Moreover, as Chaban [5] points out, aligning Ukraine's AI governance with European norms will be crucial for ensuring transparency and ethical compliance.

Ultimately, artificial intelligence should become a tool for sustainable digital transformation, not a hidden threat. When properly regulated and monitored, AI can strengthen cybersecurity, protect privacy, and contribute to rebuilding a resilient, secure, and technologically advanced Ukraine.

Bibliography:

1. Balogun, Adebayo & Metibemu, Olufunke Cynthia & Olutimehin, Abayomi & Ajayi, Adekunbi & Babarinde, Damilola & Olaniyi, Oluwaseun. The Ethical and Legal Implications of Shadow AI in Sensitive Industries: A Focus on Healthcare, Finance and Education. *SSRN Electronic Journal*. 2025. 10.2139/ssrn.5137049.

2. Vdovichena, Olha & Krymska, Anna & Koroliuk, Yurii & Shymko, Alla & Vdovichen, Anatolii. The Role of Artificial Intelligence Technologies in Rebuilding the Post-war Economy and Ensuring Cyber Security: An Example from Ukraine. *Salud, Ciencia y Tecnología – Serie de Conferencias*. 2025. № 4. 642. 10.56294/sctconf2025642.

3. Tiwo, Olufisayo & Adesokan-Imran, Temilade & Babarinde, Damilola & Salami, Isaac & Onyenaucheya, Ogechukwu & Olaniyi, Oluwaseun. Improving Patient Data Privacy and Authentication Protocols Against AI-Powered Phishing Attacks in Telemedicine. *Asian Journal of Research in Computer Science*. 2025. № 18. 93–114. 10.9734/ajrcos/2025/v18i4610.

4. Serhii Lysenko. The Role of Artificial Intelligence in Cybersecurity: Automation of Protection and Detection of Threats. *Economic Affairs.* 2024, № 69. 10.46852/0424-2513.1.2024.6.
5. Chaban Olena. Current Choices of Ukraine to the Avenues to Regulate Artificial Intelligence (AI). 2025. 10.2139/ssrn.5549841.

DOI https://doi.org/10.36059/978-966-397-570-2-97

Chiragova I.,
Postgraduate Student
National Defense University of Azerbaijan
Baku, Azerbaijan

THE INFLUENCE OF STRATEGIC CULTURE ON CYBERSECURITY POLICY FOR CRITICAL INFRASTRUCTURE

Introduction. Critical infrastructure underpins key societal functions and serves as a cornerstone for national security, economic resilience, and state governance. The prevailing understanding of critical infrastructure encompasses any network, virtual or physical asset, or system whose destruction or incapacitation would directly harm national security, public health, economic security, or safety [1]. Everyday the vulnerability is getting more expanded with a broader digitization. The significance of critical infrastructure is now evident in the prioritization of cyberattacks and associated risks by states and collective security organizations. As a result, the imperative to protect critical infrastructure compels states to develop distinct cybersecurity policies, with national approaches to risk management varying considerably. Hence, the necessity to safeguard the critical infrastructure pushes states to formulate their own cybersecurity policies, national approaches to manage the risks of which vary drastically. Futhermore, cybersecurity strategy is not merely technical, but expression of a country's vision, priorities and principles.

Usually defined as a state's ingrained habits of thought, distinct patterns of adaptation to a particular environment, set of beliefs, ideas, values symbols and etc., the concept of strategic culture shapes State's reaction towards the emerging security challenges [2, 3]. Hence, strategic culture can shape state behavior and influence the way cybersecurity policy is constructed. This paper examines whether a nation's pre-existing national strategic culture determines its choice of critical infrastructure defense model. Specifically, it investigates whether nations with historically