

Gorda GIBRADZE¹

Georgia

Sopiko GUGAVA²

Georgia

**THE IMPACT OF ARTIFICIAL INTELLIGENCE AND
CYBERSECURITY ON STATE SECURITY: EMERGING TRENDS,
RISKS, AND STRATEGIC IMPLICATIONS**

Abstract: *This study provides a comparative assessment of AI-driven cybersecurity risks in Georgia and the European Union. Employing a qualitative, policy-focused methodology, it develops a three-dimensional typology of risks encompassing infrastructure-level, information-cognitive, and strategic-geopolitical domains. The analysis draws upon authoritative policy frameworks, including the NIST AI Risk Management Framework, the EU AI Act, and Georgia’s National Cybersecurity Strategy. Findings indicate that the European Union’s advanced digital integration enhances operational capabilities but increases systemic exposure, whereas Georgia’s limited technological adoption mitigates large-scale risk while heightening vulnerability to external and hybrid threats. The study underscores that the effective integration of AI into national security frameworks necessitates robust governance, ethical oversight, and strategic coordination. By proposing a structured analytical framework, this research contributes to understanding AI-enhanced threats in diverse institutional contexts and offers practical insights for strengthening national resilience.*

Keywords: *Georgia, European Union, Artificial Intelligence, cybersecurity, state security, comparative analysis*

¹ Gorda Gibradze, PhD in Political Science, Assistant Professor, Researcher-Analyst at the Georgian Institute for Strategic and Euro-Atlantic Studies, e-mail:gibradzegorda@gmail.com

² Sopiko Gugava, Lawyer, Co-founder of She Leads Peace, Inc. (United States), Co-founder of Foreign Trained Lawyers Association (United States), Co-founder of Verston Global, Inc. (United States), LLM, Chicago-Kent College of Law, Global Business & Financial Law, Master’s, Monroe University, Criminal Justice/Law Enforcement & Homeland Security, e-mail: Sopikogugava@gmail.com

Artificial Intelligence and Cybersecurity: the EU and Georgia

Integrating AI into state security is not just technological but also geopolitical, strategic, and ethical. AI transforms threats, speeds decision-making, and raises issues of privacy and democratic oversight³. In the European Union, advanced digital integration and strong regulations enhance cybersecurity, intelligence, and crisis management. AI enables predictive modeling and rapid threat response, but high connectivity increases exposure to cyberattacks, AI-driven disinformation, and algorithmic risks. Balancing technology with oversight under the EU AI Act is crucial. In **Georgia**, limited digital integration reduces large-scale systemic risks but increases vulnerability to external and hybrid threats, including state-sponsored cyber operations and disinformation campaigns. Institutional capacity for AI governance is still developing, making international cooperation and adherence to frameworks like NIST AI RMF vital for resilience. Overall, cyberspace is a strategic arena for both Georgia and the EU. AI amplifies both offensive and defensive challenges, making cybersecurity a core pillar of state security. Sustainable policies and regulatory frameworks are essential to manage AI risks while safeguarding democratic and legal principles.

How Cybersecurity Works in the European Union

In the European Union, cybersecurity is organized across multiple levels, combining regulatory frameworks, technical coordination, and operational response mechanisms⁴.

Autonomous and Semi-Autonomous Systems

Key Structures

EU Agencies and Bodies

- ENISA (European Union Agency for Cybersecurity): The main EU agency supporting policy development, technical guidance, risk assessment, and coordination among member states.

³ *Understanding the Artificial Intelligence Revolution and its Ethical Implications*, <https://link.springer.com/article/10.1007/s11673-025-10427-6?utm_source> (08.04.2025); *Generative AI -* <<https://link.springer.com/article/10.1007/s12599-023-00834-7>> (09.12.2023); *A study on ethical implications of artificial intelligence adoption in business: challenges and best practices*, <<https://fbj.springeropen.com/articles/10.1186/s43093-025-00462-5?utmcom>> (04.03.2025).

⁴ *The EU AI Acts Interactions with Cybersecurity Legislation*, <<https://www.bsigroup.com/en-IE/insights-and-media/insights/blogs/the-eu-ai-act-and-its-interactions-with-cybersecurity-legislation>> (04.03.2025); *Artificial intelligence and cybersecurity*, <[https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762292/EPRS_ATA\(2024\)762292EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762292/EPRS_ATA(2024)762292EN.pdf)> (04.03.2025).

- CERT-EU: A specialized incident response team protecting EU institutions such as the European Parliament, the European Commission, and the Council of the EU.

EU Policy and Regulation

- NIS2 Directive: Strengthens protection of critical infrastructure and requires member states to develop national cybersecurity strategies.
- EU AI Act: Provides rules for safe and ethical AI deployment, including in security contexts.
- National Cybersecurity Strategies: Each member state creates its own strategy based on ENISA guidance (e.g., Germany, France, Spain).

Incident Response and Coordination

- CSIRT Network (Computer Security Incident Response Teams): National teams responsible for preventing, detecting, and responding to cyber threats.
- ENISA coordinates the CSIRT network, facilitating information sharing, best practices, and standardization.

Cybersecurity in Georgia

In Georgia, cybersecurity is primarily organized through national institutions and strengthened by international cooperation. While the country seeks to follow European standards, it faces several challenges due to developing technological infrastructure and institutional capacity.

Key Structures

National Coordination and Response Agencies

- Georgia's National CERT (Computer Emergency Response Team): Responsible for protecting national networks, critical infrastructure, and public institutions, detecting threats, and responding to incidents.
- State Security Service & Ministry of Internal Affairs: Oversee national cybersecurity strategy, governance, and regulatory compliance.

Strategic Documents

- National Cybersecurity Strategy 2022-2026: Defines priorities for protecting critical infrastructure, public institutions, and safe AI use.

- International standards, including NIST AI RMF and EU recommendations, are frequently referenced in policy development.

Regulatory and Legal Framework

- Legislation defines responsibilities for both public and private sectors.
- Practical aspects of GDPR are implemented for the protection of personal and organizational data.

Georgia is working to align with European cybersecurity standards and international best practices. The focus is on a risk-based, resilient system that protects critical infrastructure and cooperates with international partners. Key structures exist, but AI integration, institutional capacity, and technological modernization remain the main challenges.

Intelligent Trends in Cybersecurity

Regarding intelligent trends in cybersecurity, the field is undergoing a revolutionary transformation driven by AI⁵. These trends include the development of AI-driven Security Operations Centers (SOCs) that monitor networks, identify cyber threats, and automatically respond to cyberattacks; the creation of behavioral analytics systems that learn normal network behavior and detect anomalies or malicious activities; and the implementation of real-time threat detection models that enable immediate responses to emerging risks⁶.

These trends significantly enhance state resilience against cyberattacks, as AI systems learn from attack patterns, adapt to evolving tactics, and predict new threats. Contemporary examples include advanced countries establishing national AI-powered SOC platforms, ensuring the continuous improvement of cybersecurity systems and increasing response speed. Moreover, intelligent cyber defense increasingly relies on autonomous systems capable of assessing, responding to, and neutralizing threats with minimal human involvement⁷. Self-learning algorithms continuously acquire new knowledge from each incident, refine defensive policies, and enable the dynamic adaptation of protection mechanisms⁸. Such systems are particularly critical for state institutions, where the protection of complex and large-scale infrastructures requires uninterrupted, high-precision operations.

⁵ *Ethical Challenges Associated with the Use of Artificial Intelligence in University Education*, <https://link.springer.com/article/10.1007/s10805-025-09660-w?utm_source=com> (05.10.2024).

⁶ *Ibidem*.

⁷ *Research Integrity and Human Agency in Research Intertwined with Generative AI*, <<https://blog.scielo.org/en/2025/05/07/research-integrity-and-human-agency-in-research-gen-ai/?utmcom>> (05.07.2025).

⁸ *A Review of the Ethics of Artificial Intelligence and its Applications in the United States*, <https://arxiv.org/abs/2310.05751?utm_source=m> (10.05.2023).

Beyond strengthening defensive capabilities, intelligent trends also introduce a new class of challenges—namely, the use of AI by attackers. Cybercriminal groups and state-sponsored actors increasingly employ generative algorithms to create novel forms of malicious code, significantly complicating detection through traditional methods⁹. Personalized social engineering attacks, automated phishing campaigns, and self-directed botnets demonstrate that cybersecurity has entered an era of “AI-augmented” attacks, in which both offense and defense advance simultaneously at an accelerated technological pace. Another important dimension of intelligent cybersecurity trends relates to the reinforcement of Zero Trust architecture, which, through the application of AI, has become more dynamic and precise¹⁰. Continuous analysis of user behavior, multifactor identity management, and automated access control collectively establish a new level of security for state institutions, particularly in environments characterized by multi-layered and interconnected institutional networks. Intelligent cybersecurity trends also encompass the strengthening of algorithmic transparency, ethical regulation, and accountability. The integration of AI into state security raises sensitive issues related to data sovereignty, bias mitigation, and the legal consequences of automated decision-making¹¹. Consequently, states are increasingly developing ethical frameworks to ensure that algorithmic processes remain controllable, predictable, and aligned with democratic standards.

From a global perspective, intelligent trends are fostering new forms of international cooperation. States are seeking to develop common standards in AI-cybersecurity policy, as algorithmic evolution is intrinsically linked to the stability of the global security ecosystem. Cyber diplomacy has thus emerged as a key instrument for preventing technological escalation and for building collective defense mechanisms¹². Ultimately, intelligent trends in cybersecurity indicate that contemporary security architectures are fully dependent on advanced analytical capabilities, self-sustaining algorithms, and deep technological integration. These trends not only transform the operational environment of cyberspace but also define the long-term strategic priorities of states, in which AI has become both a source of opportunity and risk—one that requires a high level of strategic foresight and governance¹³.

⁹ *Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, And Mitigation Strategies*, <https://arxiv.org/abs/2304.07683?utm_com> (10.05.2023).

¹⁰ *How far will artificial intelligence go?*, <<https://www.lemonde.fr/en/science/article/2025/02/09/how-far-will-artificial-intelligence-go>> (02.09.2025).

¹¹ *Many organizations are already experimenting with AI agents*, <<https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai>> (03.07.2025).

¹² *Selected Papers from the International Conference on Artificial Intelligence*, <https://link.springer.com/book/9783032002310?utm_source.com> (10.05.2023).

¹³ *Critical Asset Defense with a Zero Trust Fabric*, <https://www.zentera.net/?utm_term=zero%20trust%20solution&utm_campaign=Nonbrand+Search+-+US&utm_source=>> (07.01.2024).

Conclusion

AI and cybersecurity are central pillars of contemporary state security. Predictive analytics, autonomous defense systems, and AI-driven operations expand state capabilities while imposing new ethical, strategic, and governance responsibilities. In the European Union, advanced technological infrastructure and robust regulatory frameworks provide significant security advantages. In Georgia, developing AI capabilities must be paired with international cooperation, institutional strengthening, and adherence to global standards to ensure resilience against hybrid, cyber, and geopolitical threats. A holistic, comparative understanding of AI-driven security risks is essential to safeguarding critical infrastructure, protecting public institutions, and maintaining a stable informational environment. States that effectively integrate AI with governance and ethical oversight can establish **resilient, flexible, and strategically advantaged security systems** in a rapidly evolving global landscape.

BIBLIOGRAPHY

1. *Artificial intelligence and cybersecurity*, <[https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762292/EPRS_ATA\(2024\)762292EN_pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762292/EPRS_ATA(2024)762292EN_pdf)>
2. *A study on ethical implications of artificial intelligence adoption in business: challenges and best practices*, <<https://fbj.springeropen.com/articles/10.1186/s43093-025-00462-5?utmcom>>
3. *Critical Asset Defense with a Zero Trust Fabric*, <https://www.zentera.net/?utm_term=zero%20trust%20solution&utm_campaign=Nonbrand+-Search+-+US&utm_source=>>
4. *Ethical Challenges Associated with the Use of Artificial Intelligence in University Education*, <https://link.springer.com/article/10.1007/s10805-025-09660-w?utm_source=com>
5. *Fairness And Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies*, <https://arxiv.org/abs/2304.07683?utm_com>
6. *Generative AI*, <<https://link.springer.com/article/10.1007/s12599-023-00834-7>>
7. *How far will artificial intelligence go?*, <<https://www.lemonde.fr/en/science/article/2025/02/09/how-far-will-artificial-intelligence-go>>
8. *Many organizations are already experimenting with AI agents*, <<https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai>>

9. *Research Integrity and Human Agency in Research Intertwined with Generative AI*, <https://blog.scielo.org/en/2025/05/07/research-integrity-and-human-agency-in-research-gen-ai/?utm_source=com>
10. *Review of the Ethics of Artificial Intelligence and its Applications in the United States*, <https://arxiv.org/abs/2310.05751?utm_source=m>
11. *Selected Papers from the International Conference on Artificial Intelligence*, <https://link.springer.com/book/9783032002310?utm_source=com>
12. *The EU AI Acts Interactions with Cybersecurity Legislation*, <<https://www.bisgroup.com/en-IE/insights-and-media/insights/blogs/the-eu-ai-act-and-itsinteractions-with-cybersecurity-legislation/>>
13. *Understanding the Artificial Intelligence Revolution and its Ethical Implications*, <https://link.springer.com/article/10.1007/s11673-025-10427-6?utm_source=>