

Georgia's Cybersecurity Environment in the AI Era

Abstract

This research paper explores the development of artificial intelligence (AI), international cyber threats, and Georgia's changing cybersecurity environment. This paper describes Georgia's transformation from a weak cybersecurity outpost to a nation that emphasizes promoting cybersecurity capabilities, drawing on theoretical frameworks and historical context.

Georgia experienced a paradigm shift after the 2008 cyberattack, seeing the link between cybersecurity requirements and national security. In this regard, legislative turning points were crucial in determining Georgia's cybersecurity laws. Important turning points were reached by adopting the "Law on Information Security" and ratifying the Council of Europe's cyber security convention, which laid the theoretical and practical groundwork for an all-encompassing governmental cybersecurity policy. This policy aimed to strengthen the country's national security apparatus and protect its digital infrastructure.

Georgia's efforts to strengthen its cybersecurity environment paid off over the next few years. The article details how Georgia has implemented action plans to incorporate cybersecurity concerns within the larger national security framework. Acclaim from international organizations like the International Telecommunication Union (ITU) confirmed Georgia's progress in the industry. However, the piece also gathers the ongoing weaknesses and vulnerabilities that must be addressed in the Georgian cybersecurity landscape. The cooperative endeavor yielded focused suggestions, stressing flexibility as a fundamental principle against ever-changing cyber threats.

The analysis offers valuable insights into Georgia's cybersecurity efforts and can guide other countries amidst the complex AI-driven cyber threats. The essay analyzes Georgia's strategy to defend itself against transnational cyber threats. This essay enhances knowledge of the complex interactions between transnational cyber threats and AI and the necessity of robust cybersecurity frameworks on a global scale.

Keywords: Artificial Intelligence; Cyber Security; Georgia.

¹ Researcher at Institute of Political Sciences of Ilia State University

Introduction

The relationship between the evolution of artificial intelligence (AI) and the importance of solid cybersecurity measures has become a focal point of worldwide conversation (Sarker, 2021) following the enormous technological cataclysm of the 21st century (Li, 2018). This research paper investigates this complex interaction, concentrating on Georgia's experiences.

The events of 2008 catalyzed the evolution of Georgia's cybersecurity landscape (Swanson, 2010). The orchestrated large-scale cyberattacks during the Russo-Georgian war have become a turning point, putting Georgia at the forefront of nations facing the challenges posed by malicious actors in cyberspace. Existing tensions and cyber threats forced Georgia to reevaluate the link between national security and the resilience of its digital infrastructure.

Adopting the "Law on Information Security" and the Council of Europe's cyber security convention was a turning point for Georgia's transformation in the cybersecurity space. Following the cyberattacks of 2008, these legislative achievements established the foundation for a state cybersecurity strategy. Policy positioned cybersecurity as a crucial element of national security.

In the following years, action plans were implemented, and attempts were made to incorporate cybersecurity concerns into the larger national security framework. Georgia has received international recognition for its dedication to strengthening its digital defenses. The International Telecommunication Union (ITU) ranked the nation in the top ten in the world for its 2017 Cyber Security Survey. Following the 2018 worldwide study, Georgia's inclusion in the global cybersecurity index among the top 20 nations highlighted the observable advancements in cybersecurity capabilities.

However, despite the progress, the country faced difficulties. Studies by the ITU and the E-governance Academy Estonia identified areas in Georgia's cybersecurity policy that needed improvement. With the evolution of artificial intelligence, cyberspace faced a complex perspective that highlighted the dual nature of AI in both contributing to cybersecurity improvements and facing new issues.

The chapters below will define Georgia's cybersecurity journey, examining its evaluation from vulnerability to a cyber-oriented state. It unfolds as a narrative of resilience, strategic policymaking, and international collaboration, offering a miniature version of the global conflict between technological advancements and the imperative for cybersecurity measures. Through an in-depth analysis of Georgia's experiences, this study aims to contribute to understanding the nation's unique trajectory and the broader discourse on the global stage where nations navigate the complex intersection of AI development and the imperatives of cybersecurity. This study intends to contribute to understanding Georgia's cyber policy and the global discourse on governments navigating the complex challenges of AI development and cybersecurity imperatives using an in-depth investigation of the country's experiences.

Cybercrime in the AI era

According to Andrew Ng, a British-born computer scientist and a leading thinker on artificial intelligence (AI), artificial intelligence is the new electricity (Jewell, C 2019). Understanding electricity and the invention of proper tools for its use were turning points in humankind's history (Erenoglu, 2019). With the advent of electricity and new technologies, the world has seen considerable advances in communication and production. Many scientists assume AI can become a decisive factor in the next industrial revolution (Butler-Adam, 2018). It must be seen as a means for progress, not the final product; therefore, it can be used in both directions: to serve in favor of public interests or against it. The democratization of modern technologies has made the Internet and AI available to everyone (Canaday, 2017), but at the same time, they can be used as tools for cybercrime (Sudmann, 2019).

AI can be used as an instrument for digital crime in many ways, for example:

Automated Phishing Attacks: Hackers can use AI to study and produce compelling phishing emails (Gupta, 2017). By examining the recipient's online behavior, AI can adapt the content of these emails, increasing the probability that the victim will click on harmful links or share private information.

Credential Stuffing (Ba, 2021): Attacks that include credential stuffing can be automated with AI. Hackers using machine learning algorithms can automatically use the breached username and password combinations on different websites to obtain unauthorized access.

Adversarial Attacks: To deceive machine learning models, hostile assaults manipulate input data. Hackers can trick security systems with machine-learning-based detection systems by using AI to create false samples (Qiu, 2019).

Automated Social Engineering: AI can generate highly targeted and convincing social engineering attacks by analyzing publicly available information and social media content, including building fictitious characters or chatbots to deceive people into disclosing private information (Lauinger, 2010).

AI-Powered Malware: Hackers may use AI to create and distribute complex malware that changes and adapts to protection safeguards. Malware powered by AI can adjust and learn to evade detection by conventional antivirus programs (Poudyal, 2019) .

Automated Vulnerability Exploitation: AI outperforms conventional techniques in locating and exploiting software and network vulnerabilities. Mechanical programs may swiftly analyze large datasets to identify vulnerabilities and initiate attacks (Wang, 2019).

Deepfake Attacks: Hackers can impersonate people or alter material using AI to produce convincing deepfake audio or video recordings. This can be employed to disseminate false information or focused assaults (Sharma, 2022).

It's crucial to remember that cybersecurity experts also use AI to improve security protocols and prevent these attacks. With new developments, the competition between hackers and security specialists is rising. In conclusion, cybersecurity is essential to state security in the AI era because it

shields critical infrastructure, private data, commercial interests, and democratic processes from various cyber threats.

Georgia's Cybersecurity Evolution and Shortcomings

Analyzing the state's cyber defense policy and projecting its future trajectory is crucial because, in the data age, cyber security is becoming just as vital to nations as defending their borders in the air, on land, and at sea.

Along with Estonia, Georgia was among the first nations targeted by a state-sponsored cyberattack in 2008. Unlike Estonia, Georgia was the first country against which Russia simultaneously used cyber and conventional military attacks.

Georgia's cybersecurity ecosystem evolution started in 2011. International partnerships, strategic efforts, and legislative fortifications characterized the 2011-2020. In light of the country's turbulent past, which included the noteworthy cyberattacks of 2008, Georgia decided to strengthen its cyber resilience after realizing the necessity of protecting its digital infrastructure as a part of national security.

Georgia established the framework for its cybersecurity policy in 2013, particularly with an elaboration of the Cyber Security Strategy and the Cyber Security Action Plan of Georgia – the document that defined responsible state authorities for implementing state cyber security policy. It acknowledged organizations accountable for carrying out Georgia's cybersecurity roadmap, policy, and strategy.

Georgia's cybersecurity environment was strengthened legally through specialized laws and regulations. The "Law on Information Security" adopted in 2012 established a solid legislative framework. This legislative action addressed cyber-criminal issues and set the foundation for public and private sector compliance with cybersecurity requirements.

Georgia's cybersecurity position was reinforced by legislative developments that brought it into compliance with the principles and regulations of the Budapest Convention. After adopting the mentioned document, Georgia's criminal law criminalizes unauthorized access to data, information systems, system disturbances, and device abuse.

In addition, the country has adopted the Personal Data Protection Act of 2011 to preserve human rights and freedoms when processing personal data.

Georgia proactively took part in global partnerships regarding cybersecurity cooperation. Technical teams competed against other CERT (Computer Emergency Response Team) representatives to demonstrate their cybersecurity skills. The country's technological community has actively offered training to local and foreign stakeholders and participated in several information and cybersecurity training programs.

It should be stated that Georgia also put into effect the 2017–2018 National Strategy for Cyber Security; nevertheless, the country could not create a new plan for three years after adopting the document above. Georgia's cyber security environment still faces some threats and has gaps despite the state's active efforts to improve it since 2011. These efforts included joining an international convention, approving policy documents, identifying critical information infrastructure, and setting up state structures accountable for their cyber security.

Although studies conducted by international organizations like the ITU are crucial for gaining a broad overview of the nation, these studies have the drawback of not thoroughly examining the context of the local environment.

Therefore, to analyze Georgia's cyber security environment more objectively, within the framework of this work, the key findings of the research conducted by the organization PMCG in 2021 are presented as a secondary source. According to the results of the mentioned study:

- Cybercrime is emerging in Georgia; both government and society misunderstand its threat.
- Cybercrime is likely underreported in Georgia and neighboring countries.
- MIA (Ministry of Internal Affairs) only tracks pure cybercrimes, not cyber-enabled crimes, causing ambiguity.
- Cybercrime doesn't pose significant criminal justice challenges due to its low representation in crime stats.
- Cybercrime threatens national security by converting external threats into internal issues.
- Georgian Police approach cybercrime reactively, focusing more on investigations than prevention.
- LEA (Law Enforcement Authority) faces challenges in digital forensics, especially in regions.
- Factors like lack of government policy, private sector engagement, and public awareness hinder cybercrime statistics.
- While transnational threats to Georgia's cybersecurity are minimal, GOCGs (Georgian Organised Crime Groups) may expand illegal digital activities.
- Insufficient financial support hampers key cybersecurity initiatives (PMCG, 2021).

Georgia's cyber security shortcomings were also reflected In UN ITU's Global Cybersecurity Index reports; GCI research results regarding Georgia are quoted below. Georgia in ITU reports:

2015 report (ITU, 2015) :

- *Specific legislation on cybercrime has been enacted through the following instrument: Georgia Computer System Protection Act.*
- *Specific legislation and regulation related to cybersecurity has been enacted through the following instrument: Law on Information Security.*
- *The national computer incident response teams are the CERT-GOV-GE and CERT-MOD-GOV.*
- *Georgia has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through the Law on Information Security which is based on ISO 27000.*

- *The Data Exchange Agency has an officially approved national cybersecurity framework for the certification and accreditation of public sector professionals.*
- *Georgia has an officially recognized national cybersecurity strategy (Cyber security strategy 2012-2015)*
- *The Cybersecurity strategy 2012-2015 provides a national governance roadmap for cybersecurity in Georgia.*
- *The Data Exchange Agency is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy, and roadmap.*
- *The Data Exchange Agency is currently working to measure the cybersecurity readiness of Georgia. -Georgia Computer System Protection Act.*
- *Georgia does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.*
- *The Data Exchange Agency has officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals.*
- *Georgia has 11 public sector professionals certified under internationally recognized certification programs in cybersecurity.*
- *Georgia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.*
- *Georgia does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states.*
- *Georgia has an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector through the Data Exchange Agency.*
- *Georgia has an officially recognized national or sector-specific program for sharing cybersecurity assets within the public and private sector through the Data Exchange Agency.*
- *Georgia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. CERT-GOV.GE is a member of FIRST. Georgia also participated in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014).*

2017 Report (ITU, 2017) :

“Georgia is top ranked in the CIS (Commonwealth of Independent States). After large-scale cyber-attacks on the country in 2008, the government has strongly supported protection of the country's information systems¹³. The Information Security Law¹⁴ established a Cyber Security Bureau with a particular emphasis on protecting critical information systems in the military sphere.

Georgia established cybercrime legislation in line with the principles and rules of the Budapest Convention both in terms of substantive and procedural aspects. Illegal access to information systems, data and system interference, and misuse of devices are criminalized by the Georgia criminal code. The Personal Data Protection Act was enacted by Parliament in 2011 and is intended to ensure protection of human rights and freedoms, including the right to privacy, in the course of personal data processing”.

2018 Report (ITU, 2018):

„Georgia started a cyber research project in 2018, a Portal of Online Cyber exercises⁷⁹. CyberLab – a new online resource created by Computer Emergency Response Team (CERT.GOV.GE) and Georgian Research and Educational Networking Association (GRENA) with the support of EU funded EaPConnect project. The portal helps IT students from educational institutions interested in cybersecurity to deepen their practical skills, so they can better discover and then respond to cyber incidents. The portal will also help IT personnel from both the public and private sectors, where readiness is critically important to defend against attack, ensure cyber sustainability, and improve skills. Exercises available on the portal are diverse and cover : cryptography, malware code analyses of real incidents, log file analysis of cyber incidents that occurred on real servers, reverse engineering, network flaw analyses, cyber analytics etc

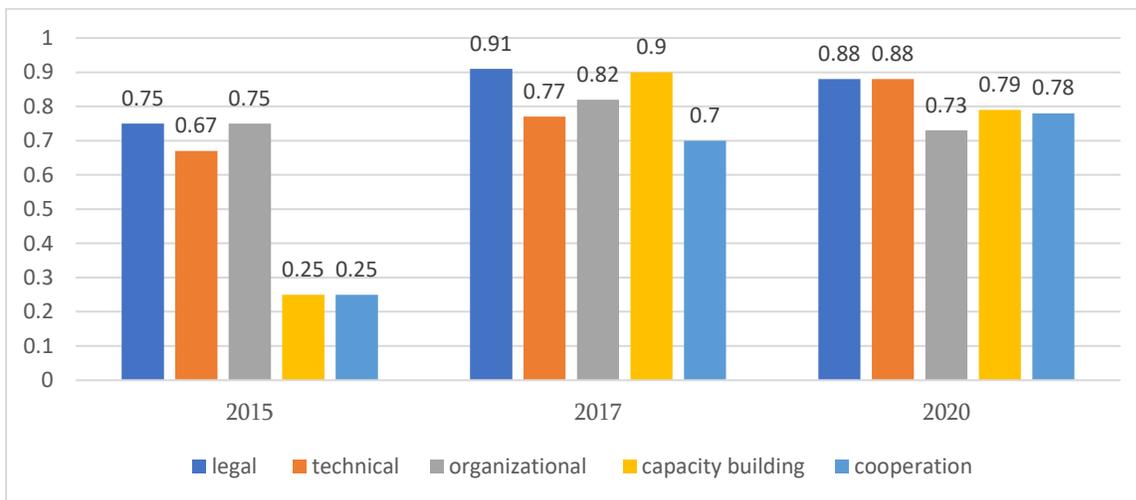
Georgia – Georgia has built up cyber capacity in-house through on-the-job training and training of teacher measures. Technical teams participate in international competitions with other CERT representatives, often successfully. In addition, the Georgia technical community provides trainings to other country stakeholders and counterparts. Representatives participate as invited experts and trainers of some international training in information and cybersecurity.“

2020 Report:

Indices were provided regarding Georgia’s Overall cybersecurity Score and its components.

Overall, the way Georgia's indicators are presented in the studies above paints the following picture (see diagram N1).

Diagram N1- Georgia's Cybersecurity index



The progress the nation made between 2015 and 2017 is depicted in detail in the above diagram, as is the stagnation brought on by the National Cyber Security Strategy's years-long implementation delay.

Conclusion

The starting point of the development of Georgia's cyber security policy was ratifying the Council of Europe's cyber security convention and enacting the "Law on Information Security. The country's standing in international studies mirrored the reforms implemented in the following years and the policy papers adopted. Yet, this progress serves as a reminder for further development rather than a place to stop.

Global and local studies also revealed weaknesses and shortcomings of the Georgian cybersecurity environment, which needs to be addressed, especially considering the ever-changing nature of cybersecurity threats.

The conclusion emphasizes the importance of flexibility in the quickly changing digital world. The suggested improvements consist of technological advancements, collaborative efforts, and legal changes, all supported by a flexible approach to cybersecurity governance. This adaptability recognizes that future challenges require solutions designed with flexibility and foresight, and it is not a one-time adjustment but a continuous process.

The journey of Georgia's cybersecurity development—from the 2008 cyberattack to its current status as a cyber-oriented nation—ends with a forceful call to action for the future.

Even though the country is currently implementing the 2021–23 state cyber security strategy, artificial intelligence is mentioned only once in the document, and that too in a general context; adding to this the fact that the state has not developed a strategy for the artificial intelligence implementation, which leaves the country vulnerable to AI-driven cybercrime.

Georgia's experience highlights how cross-border cybersecurity issues are. Coping with modern AI-driven cyber threats calls for global cooperation. The call to action goes beyond Georgia's boundaries since it acknowledges the interconnectedness of global cyber threats. It calls on researchers, cybersecurity experts, and policymakers globally to join forces to strengthen nations' overall digital resilience.

Bibliography:

- Ba, M. H. N., Bennett, J., Gallagher, M., & Bhunia, S. (2021, December). A case study of credential stuffing attack: Canva data breach. In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 735-740). IEEE.
- Butler-Adam, J. (2018). The fourth industrial revolution and education. *South African Journal of Science*, *114*(5-6), 1-1.
- Canaday, J. (2017). How the democratization of technology enhances intelligence-led policing and serves the community. *Homeland Security Affairs*.
- Erenoğlu, A. K., Erdinç, O., & Taşcıkaraoğlu, A. (2019). History of Electricity. In *Pathways to a Smarter Power System* (pp. 1-27). Academic Press.
- Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*, 3629-3654.
- International Telecommunication Union (ITU). (2015). Global cybersecurity index & cyberwellness profiles.
- International Telecommunication Union (ITU). (2017). Global Cybersecurity Index (GCI) 2017
- International Telecommunication Union (ITU). (2018). Global Cybersecurity Index (GCI)
- Jewell, C., & Ng, A. (2019). Artificial intelligence: the new electricity. *WIPO MAGAZINE*, (3), 2-6.
- Lauinger, T., Pankakoski, V., Balzarotti, D., & Kirda, E. (2010, April). Honeybot, Your Man in the Middle for Automated Social Engineering. In *LEET* (pp. 1-8).
- Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474.
- PMCG. (2021). Cybercrime in Georgia: Current challenges and possible developments. Retrieved from <https://pmcg-i.com/publication/cybercrime-in-georgia-current-challenges-and-possible-developments/>
- Poudyal, S., & Dasgupta, D. (2020, December). AI-powered ransomware detection framework. In *2020 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1154-1161). IEEE.
- Qiu, S., Liu, Q., Zhou, S., & Wu, C. (2019). Review of artificial intelligence adversarial attack and defense technologies. *Applied Sciences*, *9*(5), 909.
- Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, *2*, 1-18.
- Sharma, M., & Kaur, M. (2022). A review of Deepfake technology: an emerging AI threat. *Soft Computing for Security Applications: Proceedings of ICSCS 2021*, 605-619.
- Sudmann, A. (2019). The democratization of artificial intelligence. *Net politics in the era of learning algorithms. Transcript, Bielefeld*.

Swanson, L. (2010). The era of cyber warfare: Applying international humanitarian law to the 2008 Russian-Georgian cyber conflict. *Loy. LA Int'l & Comp. L. Rev.*, 32, 303.

Wang, Z., Zhang, Y., Tian, Z., Ruan, Q., Liu, T., Wang, H., ... & Shi, W. (2019). Automated vulnerability discovery and exploitation in the Internet of Things. *Sensors*, 19(15), 3362.