DOI:10.29013/ESR-26-1.2-10-14

INTELLECTUAL PROPERTY IN THE CYBERSECURITY STRUCTURE OF A GEORGIAN PUBLIC COMPANY. REGIMES, PRACTICES AND STRATEGIES FOR PROTECTING INTELLECTUAL PROPERTY FROM CYBER THREATS (Part 2)

Chiladze George Bidzinovich [1]

[1] J.S.D., D.B.A., Prof., University of Georgia, NASA-Georgia

Cite: Chiladze, G.B. (2026). Intellectual Property in the Cybersecurity Structure of a Georgian Public Company. Regimes, Practices and Strategies for Protecting Intellectual Property from Cyber Threats (Part 2). European Science Review 2026, No 1–2. https://doi.org/10.29013/ESR-26-1.2-10-14

Abstract

Each level of intellectual property protection from cyber threats may have its own legal regime of protection, which should ensure the necessary protection of the interests of the intellectual property owner. The article discusses the widespread threats and risks of intellectual property in the field of cybersecurity in Georgian public companies. It is important that in today's digital world, Georgian state-owned companies timely develop the best strategies for protecting intellectual property in the field of cybersecurity, taking into account relevant international practice.
Keywords: *cyber threat, intellectual property, intellectual property protection, public company*

Introduction

Special regimes for the protection of intellectual property from cyber threats include: establishing a regime for state secrets, as well as official or commercial secrets, which are based on the relevant provisions of the law (for example, the Law of Georgia "On State Secrets"). The protection of other relevant information is also provided for by the current normative acts, on the basis of which secret information, commercial information, as well as information technologies, competition, etc. are protected. (Law on State Secrets, 2025).

The protection of information containing state, official or commercial secrets (which reflects data on the protected results of intellectual activity) in a special legal regime is also provided for by the relevant articles of the Civil Code of Georgia. Protected objects containing information constituting state secrets may include: computer programs and databases; secret inventions and industrial designs; topologies of integrated circuits, etc.

As for the protection of production secrets (know-how), it is usually based on the introduction of a confidentiality regime, including a commercial secret regime. A spe-

cial legal regime for the protection of personal data is established by the Law of Georgia on Personal Data Protection and acts of the Government of Georgia concerning the requirements for the protection of personal data when processing them in information systems and the composition and content of organizational and technical measures to ensure the security of personal data when processing them in information systems (Law on Personal Data Protection, 2025).

Main text

1. Common threats and risks of intellectual property in the field of cybersecurity in Georgian public companies

The Georgian government has approved the third National Cybersecurity Strategy for 2021–2024 and its Action Plan. The current strategy focuses on two main groups of threats. These are: cyberwar, information warfare, cyberespionage, cyberattacks directed by state actors, and cybercrime, including attacks against critical infrastructures.

As stated in the document, the goal of information warfare is unauthorized access to information existed in private and public critical infrastructures of Georgia. In addition, the entities implementing critical information systems and services do not have an "appropriate level of information and cybersecurity assurance." Therefore, it is important to increase the quality of security and protection. As for cybercrime, the document lists phishing, ransomware, defacement, DDoS, and mail spoofing as the most common forms of attacks against critical infrastructures. According to the strategy, along with critical state sectors and public companies, commercial entities are increasingly becoming targets of attacks. (National Cybersecurity Strategy for 2021–2024, 2021).

Unfortunately, the document does not mention intellectual property in the field of cybersecurity at all, which, in my opinion, is a clear flaw. In addition, it does not discuss the violations common in this field – their classification is not provided.

However, for Georgian public companies, intellectual property in the field of cybersecurity refers to valuable and confidential information. It is created, stored and / or transferred by an organization or individual in the digital realm, which may include trade secrets, patents, trademarks, designs, software code, data, etc. Intellectual property in the field of cybersecurity often becomes a target of attackers when relevant persons try to steal, copy, modify or destroy it in order to gain profit or cause harm to the original owner.

It is important to discuss some common threats and risks related to intellectual property in the field of cybersecurity, which, unfortunately, are not reflected at all in the National Cybersecurity Strategy of Georgia, to indicate about how these threats and risks can affect the security, reputation and confidentiality of a public company owning intellectual property. It is also important to discuss best practices for protecting and monitoring intellectual property in the field of cybersecurity.

2. Practices and strategies for protecting intellectual property in the field of cybersecurity in public companies

It is important that state-owned companies properly understand the intellectual property values from the very beginning, in particular, the importance of their intellectual property in the field of cybersecurity and the potential impact of this property on the organization. With a correct understanding of the value, it will be possible to prioritize protection and allocate appropriate resources. It is also necessary to establish reliable controls over the organization's intellectual property in order to limit unauthorized access to it as much as possible. This includes state-owned companies: a) implementing strong authentication mechanisms, b) managing access based on roles, and c) regularly auditing it to ensure compliance. A state-owned company should ensure a secure network infrastructure – implement reliable network security measures to protect the organization's intellectual property. This should include firewalls, intrusion detection systems, and encryption protocols to protect data both during transmission and storage. At the same time, it is necessary to regularly update and improve security systems and software, including with the latest security patches, the regular use of which helps to

eliminate the causes of vulnerability and reduces the risk of unauthorized access or data leakage. (Strategies to Protect Your IP Effectively, 2024).

A separate issue is the implementation of necessary controls and timely detection of anomalies. It is important to implement advanced monitoring and anomaly detection systems to identify any unusual activity or potential violations. It is necessary to use intrusion detection and breach prevention systems, security-critical information and event management tools to proactively detect threats and respond to them.

It is important to implement secure data storage practices, including: encryption, access control, and regular creation of backups. This ensures the confidentiality, integrity and availability of the company's intellectual property, even in the event of a hacker attack or system failure. Comprehensive, effective cybersecurity incident response plans need to be developed. To test the effectiveness of the current plan, it should include defining of roles and responsibilities, establishing communication channels and conducting regular exercises. Regular audits and reviews should be conducted to identify any gaps or vulnerabilities in the company's cybersecurity practices. This includes penetration testing, vulnerability assessments and compliance audits to ensure compliance with industry standards and regulations. It is also necessary to address the issue of training employees to inform them of the importance of intellectual property in cybersecurity and their role in protecting it; In order to raise awareness, it is necessary to conduct regular trainings on potential threats, phishing attacks and social engineering methods. Finally, the company needs to be informed about the latest trends, threats and best practices in cybersecurity. It is recommended to participate in forums and conferences held within the field. It is also important to use sources of information about threats so that the company has advance information about new risks and can take proactive measures. Protecting a company's intellectual property in the area of cybersecurity requires a multifaceted, differentiated approach. By implementing these best practices and strategies, a state-owned company can improve the security of its valuable assets and reduce potential risks. (Cyber-Security Breaches, 2025).

Conclusions

1) Types of intellectual property rights violations in cyberspace, using electronic and digital means, may include: a) illegal access to information containing commercial secrets (know-how), official or state secrets, their unauthorized receipt and disclosure, including actions with prior intent ("hacking attacks"); b) unauthorized intervention in databases, creation and use of computer software to change or block information in databases with aim to replace it with other digital information (data); c) dissemination of false (inaccurate) information about a natural or legal person on the Internet, or other violation of the right to privacy, or damage to business reputation; d) violation of these rights in cyberspace, in works protected by copyright and related rights; e) illegal use of a trademark, the name of a legal entity and other means of individualization, including the illegal use of designations in domain names or in the content of web pages; f) intentional illegal use of means of individualization (commercial designation, company name, trademark, geographical indication) with the aim of causing direct or indirect harm to the copyright holder. It should be noted that the protection of intellectual property from cyber threats is usually ensured not only in relation to copyright holders with different legal statuses, but is also divided according to the levels of protection.

2) Georgia's Third National Strategy and its Action Plan focus on the following groups of threats: cyberwar, information warfare, cyberespionage, state-led cyberattacks, and cybercrime, including attacks against critical infrastructures. The goal of information warfare is unauthorized access to information in Georgia's private and public critical infrastructures. In addition, entities implementing critical information systems and services do not have "an appropriate level of information and cyber security." Therefore, it is important to improve the quality of security and protection. As for cybercrime, the document lists phishing, ransomware, defacement, DDoS, and mail spoofing as the most common forms of attacks against

critical infrastructure. Unfortunately, the document does not address intellectual property in the field of cybersecurity at all, which is a clear shortcoming. In addition, it does not discuss the violations common in this field and it does not provide a classification. Intellectual property in the field of cybersecurity is often targeted by attackers, when certain parties attempt to steal, copy, modify, or destroy it for profit or to cause harm to the original owner. It is important to discuss some of the common threats and risks related to intellectual property in the field of cybersecurity, which, unfortunately, are not reflected at all in the National Cybersecurity Strategy of Georgia, to indicate/explain as how they can affect the security, reputation and confidentiality of a public company that owns intellectual property.

3) It is important that Georgian state-owned companies develop the best strategies for protecting intellectual property in the field of cybersecurity in a timely manner, take into account relevant international practices, and correctly understand from the outset the importance of their intellectual property in the field of cybersecurity and the potential impact of this property on the organization. With a correct understanding of the value, it will be possible to rank protection priorities and allocate appropriate resources. It is also necessary to establish reliable control over the organization's intellectual property in order to limit unauthorized access to it as much as possible. This includes state-owned companies: a) implementing strong authentication mechanisms, b) managing access based on roles, and c) conducting regular audits to ensure compliance. A state-owned company should ensure a secure network infrastructure – implement reliable network security measures to protect the organization's intellectual property. Firewalls, intrusion detection systems, and encryption protocols should be used to protect data both in transit and when stored. Security systems and software should be regularly updated and refined, including with the latest security patches, the regular use of which helps eliminate the causes of vulnerability and reduces the risk of unauthorized access or data leakage. It is important to implement advanced monitoring and anomaly detection systems to identify any unusual activity or potential violations. It is necessary to use intrusion detection and breach prevention systems, security-critical information, and event management tools in order to proactively detect threats and respond to them. It is important to implement secure data storage practices. Comprehensive, effective plans for responding to cybersecurity incidents need to be developed. To test the effectiveness of the current plan, it should include defining roles and responsibilities, establishing communication channels, and conducting regular exercises. Regular audits and reviews should be conducted to identify any gaps or vulnerabilities in the company's cybersecurity practices. This includes system penetration testing, vulnerability assessments, and compliance audits. It is also necessary to address the issue of employees' training. The company needs to be informed about the latest cybersecurity trends, threats, and best practices.

References

Law of Georgia on State Secrets (2025). URL: https://mod.gov.ge/uploads/public/_%E1%83%90%E1%83%A5%E1%83%A2%E1%83%94%E1%83%91%E1%83%98/saxelmwifo_saidumloebis_shesaxeb_saqartvelos_kanoni.pdf

Law of Georgia on Personal Data Protection (2025). URL: https://pdps.ge/files/content/%E1%83%9E%E1%83%94%E1%83%A0%E1%83%A1%E1%83%9D%E1%839C%E1%83%90%E1%83%9A%E1%83%A3%E1%83%A0%20%E1%83%9B%E1%83%9D%E1%83%9C%E1%83%90%E1%83%AA%E1%83%94%E1%83%9B%E1%83%97%E1%83%90%20%E1%83%93%E1%83%90%E1%83%AA%E1%83%95%E1%83%98%E1%83%A1%20%E1%83%A8%E1%83%94%E1%83%A1%E1%83%90%E1%83%AE%E1%83%94-%E1%83%91%20%E1%83%9B%E1%83%9D%E1%83%A5%E1%83%9B%E1%83%94%E1%83%93%E1%83%98%20%E1%83%99%E1%83%90%E1%83%9C%E1%83%9D%E1%83%9C%E1%83%98_1711019935.pdf

Georgia approved the National Cybersecurity Strategy for 2021–2024 (2021). URL: https://civil.ge/ka/archives/446832
Strategies to Protect Your Intellectual Property Effectively (2025). URL: https://www.zoppi.co.uk/blog/strategies-to-protect-your-intellectual-property-effectively
Cyber-Security Breaches (2025). URL: https://www.dataguard.com/cyber-security/breaches/

submitted 28.12.2025;
accepted for publication 14.01.2026;
published 28.02.2026

Contact: dr.chiladze@gmail.com