European Science Review 2025,
No 11–12
ISSN 2310-5577

PREMIER Publishing
ppublishing.org

DOI:10.29013/ESR-25-11.12-22-25

INTELLECTUAL PROPERTY IN THE CYBERSECURITY STRUCTURE OF A GEORGIAN PUBLIC COMPANY. REGIMES, PRACTICES AND STRATEGIES FOR PROTECTING INTELLECTUAL PROPERTY FROM CYBER THREATS (Part 1)

Chiladze George Bidzinovich [1]

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

Cite: *Chiladze, G.B. (2025). Intellectual Property in the Cybersecurity Structure of a Georgian Public Company. Regimes, Practices and Strategies for Protecting Intellectual Property from Cyber Threats (Part 1). European Science Review 2025, No 11–12.* https://doi.org/10.29013/ESR-25-11.12-22-25

Abstract.

The institution of intellectual property occupies one of the most important places in Georgian legislation. The results of intellectual activity, goods, works, services and means of individualization of legal entities of public law, which are granted legal protection by law and which are defined as intellectual property according to the Civil Code of Georgia and special laws, are intangible assets with material, commodity value.

Patents issued for inventions, utility models, industrial designs, as well as trademarks, computer programs and copyrighted works, production secrets (know-how) and other intellectual intangible assets - which contain innovative technical and humanitarian knowledge and skills - acquire special value for public companies that own their rights in the context of global market relations.

Keywords: *intellectual property, public company, cyber threat, intellectual property protection*

Introduction

For public companies, information (data) about the nature and content of innovative achievements is extremely important in today's highly competitive environment. This is essential regardless of whether the content of such intangible assets is accessible to an unlimited number of persons (for example, a description of an invention in a patent application, a conditional designation of a trademark, a published work of the author, etc.), or information about advanced development technologies is "covered" by commercial secrets (know-how) or protected by state secrets. Georgian legislation ensures the protection of rights to such intangible assets in favor of their rights holders. (Challenges IP in Global Market, 2024).

The use of patents, trademarks, computer programs and other intellectual property objects in civil circulation and commodity circulation is allowed subject to the exclusive right of their legal owner. The forms of such use are very diverse and include both direct

use and the use of the results of intellectual activity and means of individualization in goods in civil circulation and placed on the market.

Main text

1. What is cybersecurity intellectual property and why is it important in the public sector?

Cybersecurity intellectual property is used to describe valuable and unique information, ideas, inventions, and innovations created, owned, or used by individuals or organizations involved in cybersecurity. Cybersecurity intellectual property may include software code, algorithms, patents, trade secrets, designs, methods, processes, data, and know-how related to the creators and owners of cybersecurity intellectual property, its detection, or response. (IP in Cyberspace, 2025).

For state-owned companies, intellectual property in the field of cybersecurity is important for several reasons: 1) it provides a competitive advantage to creators and owners of intellectual property in the field of cybersecurity; 2) it helps differentiate the products, services and solutions offered by companies, researchers and professionals operating in the field of cybersecurity from their competitors; 3) it can attract customers, investors and partners who value the quality, reliability and innovation of intellectual property in the field of cybersecurity; 4) it promotes the creation and development of new and improved intellectual property in the field of cybersecurity; 5) it can be a source of income, recognition and rewards for creators and owners of such property; 6) It may also encourage them to attract and invest more time, money and other necessary resources in the development and improvement of cybersecurity intellectual property, which will benefit the cybersecurity industry and society as a whole; 7) Protects the rights and interests of creators and owners of cybersecurity intellectual property; 8) Can help prevent unauthorized use, disclosure, copying, modification or theft of intellectual property protected by the cybersecurity regime by others who may attempt to exploit, damage or otherwise impair the cybersecurity intellectual property or its creators and owners; 9) Can help ensure that users and intellectual property licensees fulfill their legal, contractual obligations and responsibilities in the field of cybersecurity. (legal advantage, 2025; Domination of Cybersecurity, 2023).

2. Cyber threats and intellectual property rights. Violations of intellectual property rights in Georgian public companies

In relation to intellectual property, cyber threats are associated with the risk of infringement of intellectual rights to the relevant objects. Risk, – as a certain probability of negative consequences, – in relation to intellectual property is expressed in the possibility of infringement of intellectual rights (primarily, special / exclusive rights) with varying degrees of probability. Infringement of intellectual property rights implies the illegal use of the result of intellectual activity or means of individualization, which leads to damage to the public company holding the copyright in the form of lost / unearned income or damage to its reputation (image).

In a public company, infringement of intellectual property rights recorded on its balance sheet can be expressed, for example: 1) by infringement of patented technical solutions, – on the basis of its direct use by third parties, – in the production of a product; 2) It may be associated with the illegal use of a patented method. Indirect infringement of intellectual property rights occurs when counterfeit products (goods) are released into civil circulation or otherwise introduced there. The effectiveness of intellectual property rights protection in the digital space of the Internet is determined by the ability to resist such violations and the threats arising from them. Threats of infringement of intellectual property rights in cyberspace (cyber threats) are associated with certain risks and may affect the physical existence of the object containing the relevant rights. In particular, as a result of cyber attacks, certain databases containing commercially valuable information may be modified or completely lost, or information containing trade secrets may be disclosed, which leads to the loss of confidentiality and the termination of rights to production secrets (know-how), in accordance with the established procedure. (What is IP Infringement?, 2023).

Violations of intellectual property rights in the digital space of the Internet as a result of cyberattacks / cyberthreats have their own specifics. In particular, the types of violations of intellectual property rights in cyberspace – using electronic and digital means – may include: 1) 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"); 2) unauthorized intervention in databases, creation and use of computer software to change information in databases or block it and replace it with other digital information (data); 3) 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; 4) violation of these rights in cyberspace, on works protected by copyright and related rights; 5) 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; 6) 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. (I.Sopilko and others, 2023; D.Bennet & Ludwig, 2024).

It should be noted that, in accordance with the legislation in force in the country, the owner of patents, trademarks, know-how, integrated circuit topologies, computer programs, copyrighted works and other relevant objects of intellectual property can be both a private individual and an organization, as well as the state and its entities. In this regard, the protection of intellectual property from cyber threats, as a rule, is ensured not only in relation to copyright holders with different legal statuses, but is also divided according to the levels of protection.

Conclusions

1) Intellectual property in the field of cybersecurity is important for Georgian state-owned companies for several reasons: it provides a competitive advantage to creators of intellectual property in the field of cybersecurity and its owners; it helps to differentiate the offered products, services and solutions from competitors; Can attract users, investors and partners who value the quality, reliability and innovation of cybersecurity intellectual property; Promotes the creation and development of cybersecurity intellectual property and can be a source of revenue, recognition and reward, as well as a source of protection and encouragement for relevant individuals; Can help prevent unauthorized use, disclosure, copying, modification or theft of cybersecurity-protected intellectual property by others; Can help ensure that users and intellectual property licensees comply with their legal, contractual and responsibilities in cybersecurity.

2) In a public company, the risk in relation to intellectual property is expressed in the possibility of violation of intellectual rights (primarily special / exclusive rights) with varying degrees of probability. Violation of intellectual property rights implies the illegal use of the result of intellectual activity or means of individualization, which causes damage to the public company holding the copyright in the form of lost / unearned income or damage to its reputation (image).

In a public company, violation of intellectual property rights recorded on its balance sheet may be expressed, for example: a) in violation of the law of patented technical solutions, – on the basis of its direct use by third parties, – in the production of a product; b) it may be associated with the illegal use of a patented method. Indirect infringement of intellectual property rights occurs when counterfeit products (goods) are released into civil circulation or otherwise introduced into it. As a result of cyberattacks, certain databases containing commercially valuable information may be modified or completely lost, or information containing trade secrets may be disclosed, which leads to the loss of confidentiality and the termination of rights to production secrets (know-how), in accordance with the established procedure.

References

Challenges of Intellectual Property in the Global Market (2024) URL: https://online.mountsaintvincent.edu/degrees/business/mba/international-business/intellectual-property-challenges/

Intellectual Property in Cyberspace (2025). URL: https://www.geeksforgeeks.org/ethical-hacking/intellectual-property-in-cyberspace/

Cybersecurity and Intellectual Property The Rising Importance of Patents in Protecting Innovation, (2025) URL: https://legaladvantage.net/2025/02/cybersecurity-and-intellectual-property-the-rising-importance-of-patents-in-protecting-innovation/

The Domination of Cybersecurity (2023) URL: https://www.pietragallo.com/blog/the-domination-of-cybersecurity/

What is IP Infringement? (2023) URL: https://www.digitalguardian.com/blog/intellectual-property-infringement

Iryna Sopilko, Valeriia Filinovych, Liliia O. Pankova, Serhii V. Obshalov

Kostiantyn O. Chaplynskyi. (2023). Protection of Intellectual Property Rights from Cyber Threats in the Global Information Environment URL: https://novumjus.ucatolica.edu.co/index.php/Juridica/article/view/4582/4709

Dunlap Bennett & Ludwig. (2024). How IP Law and Cybersecurity Intersect. URL: https://www.dbllawyers.com/intellectual-property-law-cybersecurity/

submitted 12.12.2025;
accepted for publication 26.12.2025;
published 30.12.2025

Contact: dr.chiladze@gmail.com