DOI: https://doi.org/10.30525/2256-0742/2025-11-1-301-307

INTERNATIONAL LEGAL MECHANISMS FOR COMBATING CYBERCRIME: THE ECONOMIC IMPACT ON AZERBAIJAN AND GLOBAL PRACTICES

Gulnaz Aydin Rzayeva[1]

Abstract. The purpose of this study is to examine the impact of cybercrime on the economy of Azerbaijan and to assess the international legal mechanisms for combating these threats. This paper highlights the economic impact of cybercrime, in particular on GDP, business operations, financial security and foreign direct investment (in the Azerbaijani context). Utilising historical, comparative, and policy analysis methodologies, this study examines Azerbaijan's strategies (including national cybersecurity investments and international co-operation) within the context of global best practices. The findings of the study suggest that robust legal frameworks and targeted cybersecurity initiatives are essential to mitigate financial losses from cybercrime, protect business continuity, and foster a secure climate for economic growth and investment. The study emphasises the necessity of incorporating economic factors into cybersecurity policy and underscores the importance of international collaboration and adherence to global conventions, such as the Budapest Convention, in enhancing Azerbaijan's economic resilience to cyber threats.

Keywords: cybercrime, economic impact, cybersecurity, digital economy, Azerbaijan, international co-operation, foreign investment.

JEL Classification: K24, F60, F50

1. Introduction

In the contemporary digital era, cybercrime has evolved into a substantial threat not only to security but also to economic stability. On a global scale, cybercriminal activities are estimated to cause enormous financial losses, reaching close to 600 billion USD per year (nearly one percent of global GDP) (Lewis, 2018). This figure surged to over 1 trillion USD by 2020 (Lewis et al., 2020). These losses can be considered a "tax on innovation", which has the effect of slowing economic growth by reducing the return on digital investments. The repercussions of cybercrime on the economy are manifold in nature. It has the capacity to undermine business operations, engender direct financial costs, erode consumer trust, and act as a deterrent to foreign investment. Azerbaijan, as a country rapidly developing its digital economy, faces mounting economic risks from cyber threats. In recent years, Azerbaijan has witnessed a notable expansion in e-government services, digital banking, and online business activities, which have contributed to an increase in GDP growth. Nevertheless, this increased digitalisation also renders the economy more vulnerable to cyber attacks. This vulnerability is evidenced by a notable increase in phishing and fraud attempts directed at Azerbaijani banks and companies, which have the potential to inflict significant financial losses. If global averages hold, cybercrime could cost Azerbaijan hundreds of millions of US dollars annually in direct and indirect damages. Beyond direct financial losses, successful cyber attacks could weaken customer confidence in digital services and stifle the country's investment climate. Recognising these dangers, the government of Azerbaijan has taken significant steps to strengthen its cyber defences through legislative reforms and strategic initiatives. The country is a signatory to several key international agreements, including the Council of Europe's Budapest Convention on Cybercrime, which serves to align its national legislation with global standards. Furthermore, a National Strategy on Information Security and Cybersecurity (2023–2027) has been initiated, with the objective of integrating cybersecurity into its broader economic development goals.

[1] Baku State University, Azerbaijan
E-mail: Gulnazrzayeva@mail.ru
ORCID: https://orcid.org/0000-0001-5305-7113

These efforts are indicative of an awareness that combating cybercrime is not only a law enforcement necessity but also an economic imperative. The present article examines international legal mechanisms for combating cybercrime, with a particular focus on their relevance to Azerbaijan's economic security. The analysis examines the adaptation of global frameworks and best practices in cybercrime prevention in Azerbaijan, and the impact of cybercrime on the nation's economy in terms of GDP, business continuity, financial sector stability, foreign direct investment (FDI), and economic policy. The study employs a combination of historical analysis, comparative review and policy analysis to evaluate the effectiveness of current measures and identify gaps. By focusing on both legal and economic dimensions, the paper seeks to offer a holistic view of Azerbaijan's experience in dealing with cybercrime and to propose insights for strengthening economic resilience against cyber threats.

2. Literature Review

A substantial corpus of literature has explored the multifaceted impacts of cybercrime on national and global economies. Lewis (2018) and Lewis et al. (2020) provide foundational statistics highlighting cybercrime's severe financial toll globally, quantifying annual losses into the hundreds of billions. Arnell and Faturoti (2023) critically evaluate jurisdictional challenges that arise in prosecuting cybercriminals across borders, emphasising implications for global economic stability. In their 2021 analysis, Kastner and Mégret (2021) emphasised the necessity for harmonised global cybersecurity standards in order to protect economic infrastructures, whilst also conducting an analysis of the international legal dimensions.

Dharminder et al. (2023) and Didkivska and Shevchenko (2023) provide insights into the international and national legal mechanisms combating cybercrime, emphasising their critical role in securing digital economies. Buçaj and Idrizaj (2024) advocate for enhanced global legal regulations, recognizing cybercrime as a barrier to sustainable economic development. In their 2018 publication, Donalds and Osei-Bryson (2018) propose an ontological framework with the aim of facilitating the classification of cybercrimes. This structured approach is of benefit to economic policy-makers.

In the context of regional research, Akhundov's (2023) study on Azerbaijan emphasises the national cybersecurity strategies, underscoring substantial investments aimed at safeguarding economic activities. Balajanov (2017) evaluates the effectiveness of Azerbaijan's law enforcement against cybercrime, revealing both successes and areas requiring improvement. Spînu (2020) provides a further discussion of cybersecurity governance in Azerbaijan, highlighting policy gaps that have the potential to impact economic confidence and security. Additionally, Samedova Sh.T. (2020), a leading expert in the field of criminal law, has undertaken research on cybersecurity crimes in Azerbaijan.

Further economic perspectives from Kopp et al. (2017) delineate the systemic financial risks posed by cyber threats, which are pertinent to Azerbaijan's emerging digital banking sector. Li and Stephenson (2024) discuss the necessity of aligning digital growth with cybersecurity, reinforcing the direct relationship between cyber resilience and foreign investment attractiveness. Finally, Alazraq (2021) explores legislative approaches in the digital age, informing comparative analyses relevant to Azerbaijan's evolving economic policies.

Collectively, these studies provide a robust foundation for further discussion in the context of Azerbaijan's economic security, underpinning the economic significance of robust cybersecurity frameworks and international co-operation.

3. The Main Research Material

Global Economic Impact of Cybercrime

Cybercrime has become a costly global economic problem. Studies by international research institutions show that the global cost of cybercrime has risen sharply. The Center for Strategic and International Studies (CSIS) reported a jump in annual global cybercrime losses from an estimated 445 billion USD in 2014 to around 600 billion USD in 2018 (about 0.8% of global GDP). A joint report by McAfee and CSIS found that by 2020, global losses will exceed 1 trillion USD, or just over 1 percent of global GDP (Lewis et al., 2020). These figures include theft of financial assets and intellectual property, fraud, ransomware payments, and the many costs associated with responding to incidents. If cybercrime were measured as an economy, its 'GDP' would be equivalent to that of a medium-sized country, underlining the severity of its impact on economic activity. In addition to total losses, cybercrime imposes significant indirect costs on economies. It disrupts business operations through system downtime and lost productivity. A 2020 survey found that around two-thirds of affected companies experienced operational downtime due to cyber incidents, with the average cost of the longest downtime event being 762,000 USD. Such disruptions result in lost output and efficiency, which can ripple through supply chains. Furthermore, a survey of companies revealed that 92% of those affected by a cyber attack reported adverse consequences that extended beyond immediate financial losses. These consequences included reputational damage and erosion of customer trust.

These hidden costs can damage a country's economic prospects by reducing consumer confidence in digital services and forcing businesses to divert resources to security and recovery efforts. Cybercrime also acts as a drag on innovation and investment. It has been called a de facto "tax on innovation" as companies are forced to spend more and more money on cybersecurity and incident recovery measures, funds that could otherwise be used for productive investment or research and development. Theft of intellectual property through cyber espionage can undermine competitive advantage and hinder innovation, particularly in technology-based industries. From a macroeconomic perspective, high rates of cybercrime have the potential to act as a deterrent to foreign investment, as potential investors may hesitate to enter markets perceived as having weak cybersecurity, fearing that their capital or proprietary information could be at risk. In summary, the growth of cybercrime worldwide poses a significant challenge to economic growth, demanding that nations integrate cybersecurity considerations into their economic policies.

Cybercrime and Economic Security in Azerbaijan

Azerbaijan's increasing digitalisation has brought economic opportunities, but also increased cyber risks. The country has invested in its digital infrastructure and promoted online services in banking, commerce and government. As a result, the digital economy has become an important contributor to overall economic development. However, this also means that cyber threats have a greater potential to affect national economic security. Recent trends indicate that Azerbaijan is facing a growing number of cyber incidents. According to data from Kaspersky, approximately one million phishing attacks were thwarted in Azerbaijan in 2022 alone, with approximately 40% of these attacks targeting corporate users. This high rate of attacks on businesses suggests a direct threat to corporate financial assets and operations. The prevalence of online banking fraud and scams, which aim to steal payment data, is also of concern. If left unchecked, these issues have the potential to erode public trust in the banking system and e-commerce. The financial sector in particular illustrates the stakes for economic security. Azerbaijan's banking industry has rapidly expanded digital services, including mobile banking and cashless payment systems. While these innovations improve efficiency and contribute to GDP growth, they also become prime targets for cybercriminals. A successful breach of a major bank could not only result in the theft of money, but also destabilise financial markets and reduce public confidence in the financial system. Recognising this, Azerbaijani regulators have introduced strict cybersecurity requirements for banks. In April 2022, the "Rules for Information Security Management in Banks" came into force, setting minimum cybersecurity standards for financial institutions. In addition, the Central Bank of Azerbaijan approved a dedicated "Cybersecurity Strategy in Financial Markets for 2023-2026" to create a sustainable cyber defence environment in the financial sector. The objective of these measures is to protect the integrity of online banking and payment systems, thereby ensuring the stability of a critical pillar of the economy. It is important to note that cyber threats in Azerbaijan are not limited to the financial sector. Other industries, including but not limited to energy, telecommunications, and e-government services, are also vulnerable to cyber threats. The energy sector, a pivotal driver of the Azerbaijani economy, is reliant on intricate industrial control systems that are susceptible to cyber sabotage or espionage. Furthermore, government digital services and databases contain sensitive information, and a breach could result in significant disruption to public services and substantial recovery costs. The repercussions of a significant cyber incident in any of these sectors could be considerable, potentially impacting foreign trade (for instance, if energy exports were to be disrupted) or resulting in costly periods of downtime. In addition, large-scale cyber attacks linked to geopolitical conflicts (such as the reported attacks on Azerbaijani institutions during regional conflicts) highlight that cyber threats can have macroeconomic implications, potentially requiring the redirection of government spending towards response and resilience. Awareness of the economic impact of cybercrime has grown in Azerbaijan's public and private sectors. Companies are increasingly investing in cybersecurity solutions and training to protect their assets. However, gaps in cyber preparedness still exist, especially among small and medium-sized enterprises (SMEs) that have more limited resources. Many SMEs form the backbone of the economy, and their cumulative losses from cybercrime (through fraud, ransomware or compromised business emails) can add up and indirectly affect economic performance (e.g., through higher insurance premiums or credit risks). As such, strengthening cybersecurity at all levels of the economy has become a strategic concern for Azerbaijan, beyond just an IT or law enforcement issue.

International Legal Mechanisms and Co-operation

Effectively combating cybercrime, particularly to protect economic interests, requires a robust legal framework and international co-operation. Azerbaijan's legal and institutional approach to cybercrime has been significantly shaped by international mechanisms. The Council of Europe's Convention on Cybercrime (Budapest Convention) is of primary significance in this regard, and Azerbaijan acceded to it in 2009. By acceding to this convention, Azerbaijan committed to criminalising a range of cyber offences (such as unauthorized access, data interference, system

interference, and computer-related fraud) in line with internationally recognised standards. The Convention establishes protocols for cross-border co-operation, empowering Azerbaijani authorities to request and exchange electronic evidence with foreign nations. This is of particular importance in cases where cybercrimes affecting the economy of Azerbaijan (for example, transnational fraud schemes or attacks originating abroad) involve perpetrators or infrastructure in foreign jurisdictions. In addition to the Budapest Convention, Azerbaijan aligns with other global and regional initiatives. The country has been following the developments in the United Nations' efforts to draft a comprehensive international cybercrime treaty, perceiving it as an opportunity to strengthen global collaboration in law enforcement. Azerbaijan is also a member of the Commonwealth of Independent States (CIS) Agreement on co-operation in combating offences in the sphere of computer information (2008), which facilitates regional coordination among post-Soviet states. These affiliations reflect Azerbaijan's understanding that cyber threats transcend borders, and that harmonisation of legal approaches is essential to tracking and prosecuting cyber criminals targeting the country's economy. International law enforcement co-operation through organisations such as INTERPOL and Europol is of practical importance to Azerbaijan. Despite not being an EU Member, Azerbaijan benefits from co-operation with Europol on cases that have a European dimension. Likewise, INTERPOL's global cybercrime programmes assist Azerbaijan in receiving alerts about novel cybercrime tactics and in coordinating cross-border investigations. For instance, in the event of a major financial cyber fraud affecting an Azerbaijani bank that involves money mules or command-and-control servers in other countries, channels established by these international mechanisms enable timely information exchange and possible retrieval of stolen assets. Such co-operation can significantly reduce the economic damage by increasing the chances of catching perpetrators and recovering funds. At the policy level, alignment with international legal mechanisms provides Azerbaijan with a framework for updating its domestic legislation. The country has regularly amended its Criminal Code to include cybercrime offences and penalties recommended by international instruments. It has also worked to improve procedural laws to allow lawful access to digital evidence, while respecting privacy and human rights standards. By harmonising laws with partners, Azerbaijan is making it easier for multinational companies to operate safely on its territory, knowing that there are clear legal remedies for cyber incidents. However, challenges remain in making full use of international mechanisms. Differences in legal standards and the slow pace of mutual legal assistance can hinder swift action, sometimes allowing cybercriminals to exploit jurisdictional gaps. Moreover, not all countries from which cyber attacks may originate are equally committed to co-operation. Despite these hurdles, Azerbaijan continues to advocate for a stronger international framework, recognising that a secure cyberspace is a shared global good necessary for stable economic development.

Azerbaijan's National Response and Cybersecurity Investments

Azerbaijan has been proactively strengthening its national cyber defences to protect its economy and citizens. A cornerstone of these efforts is the National Strategy on Information Security and Cybersecurity for 2023-2027. This strategic document outlines a comprehensive approach to cybersecurity, emphasising both technological and organisational measures. Crucially, it frames cybersecurity as part of Azerbaijan's development strategy to 2030, ensuring that investments in cyber defence are seen as investments in economic sustainability. As part of the National Strategy, Azerbaijan is establishing clearer governance structures for cybersecurity. An Information Security Coordination Commission will be established to oversee policy implementation across government agencies. Specialised cybersecurity units are being established within government institutions, and public-private partnership platforms are planned to facilitate risk assessment and information sharing between government and industry. Such coordination is expected to improve incident response and resilience, minimising economic disruption from cyber attacks on critical infrastructure. Investment in human capital is another key component. In March 2023, Azerbaijan launched the Azerbaijan Cybersecurity Centre in partnership with Israel's Technion Institute and a large private conglomerate (PASHA Holding). The centre is tasked with training more than 1,000 cybersecurity professionals over the next few years, equipping them with the skills to tackle evolving cyber threats. This initiative addresses the cybersecurity skills shortage and is expected to benefit companies that can hire local experts instead of relying solely on external consultants. In March 2023, Azerbaijan launched the Azerbaijan Cybersecurity Centre in partnership with Israel's Technion Institute and a large private conglomerate (PASHA Holding). The centre is tasked with training more than 1,000 cybersecurity professionals over the next few years, equipping them with the skills to tackle evolving cyber threats. This initiative addresses the cybersecurity skills shortage and is expected to benefit companies that can hire local experts instead of relying solely on external consultants. The country is also implementing an electronic law enforcement information system called "Cybercrime", which will help track and manage cybercrime cases more

efficiently. Such a system can speed up investigations and reduce the window of opportunity for cybercriminals, thereby mitigating potential losses. Economic incentives have been introduced to encourage cybersecurity practices in the private sector. The Information Security Strategy calls for consideration of tax incentives and other benefits for companies that invest in cybersecurity technologies and solutions. Such incentives reduce the financial burden on businesses to implement robust security measures, effectively acting as a subsidy to reduce cyber risk. Over time, as businesses become more secure, the frequency and severity of successful attacks across the economy should decrease, preventing losses that would otherwise have occurred. Azerbaijan's efforts also extend to raising public awareness and building a culture of cyber hygiene, which is essential for economic security. Government agencies and banks regularly issue warnings about common scams (such as phishing emails or fraudulent SMS messages) to educate users. By fostering a more cyber-aware population, Azerbaijan aims to reduce the success rate of attacks that exploit human error, such as social engineering tactics. This is particularly important for protecting the finances of individuals and the cumulative impact on the economy (the fewer people who fall victim to cyber fraud, the less household wealth is lost and the less law enforcement resources are reduced).

Foreign Investment and International Collaboration

Cybersecurity has increasingly become a factor in Azerbaijan's attractiveness to foreign investors. A secure digital environment is essential for attracting businesses in the technology, finance and e-commerce sectors. Investors typically conduct risk assessments before entering a market, and a high incidence of cybercrime or weak legal protection can raise red flags. In the context of FDI, cybersecurity is intertwined with the ease of doing business: a reliable digital infrastructure and strong data protection laws make a country more attractive for investment. Analysts have indicated that concerns pertaining to the theft of intellectual property and inadequate cybersecurity may prompt investors to reevaluate their market entry intentions, as they apprehend potential financial losses or espionage. Conversely, countries that demonstrate robust cybersecurity frameworks signal to investors that their operations and intellectual assets will be safer. Azerbaijan's collaboration with international bodies serves to provide reassurance to investors. By collaborating with organisations such as the World Economic Forum (WEF) on digital economy initiatives, Azerbaijan demonstrates its commitment to global best practices. A 2024 WEF report highlighted the necessity of bridging the gap between rapid ICT growth and slower progress in cybersecurity development for the purpose of improving business confidence (Li & Stephenson, 2024). The report posited that countries with robust cybersecurity policies are more appealing to both domestic and foreign investors. Azerbaijan's ongoing reforms, including the updating of its cybersecurity legislation to encompass critical infrastructure, the alignment of domestic policy with EU directives where feasible, and the active participation in international cybersecurity indices, contribute to the enhancement of its reputation as a secure place to conduct business. International collaboration projects, such as adhering to EU ENISA guidelines or engaging with NATO's Co-operative Cyber Defence Centre of Excellence (CCDCOE) for knowledge-sharing, provide Azerbaijan with advanced know-how that can translate into better security for its digital economy. Although Azerbaijan is not a NATO member, it benefits from partnerships and exercises that improve preparedness against cyber threats (e.g., sending observers to NATO cyber defence exercises or participating in EU Eastern Partnership cybersecurity capacity programmes). These collaborations often focus on the protection of critical infrastructure and financial systems, directly supporting economic stability. In addition, Azerbaijan has sought assistance from countries with advanced cybersecurity expertise (such as Estonia and Israel) to audit and strengthen its cyber defences. Such global co-operation enhances Azerbaijan's ability to prevent large-scale incidents that could have cross-border economic impacts, such as attacks on oil and gas infrastructure or international banking networks. Finally, Azerbaijan's commitment to international standards is reflected in its improved ranking in cybersecurity indices. It has risen to 40th place out of 194 countries in the International (Akhundov, 2023). This rise in rankings is not only a matter of national pride, but also an important signal to the global business community that Azerbaijan is strengthening its cyber governance. Over time, sustained improvement in such indices can correlate with increased foreign investment, as businesses become more confident in the stability and security of the business environment. In this way, Azerbaijan's international co-operation on cyber issues is an investment in its economic future, reducing the risk that cybercrime will undermine the country's development goals.

4. Conclusions

Cybercrime poses a significant threat to the economic well-being of nations, and Azerbaijan is no exception. This study highlights that protecting Azerbaijan's economy requires an integrated approach that combines strong international legal mechanisms with national strategies focused on economic resilience. Internationally, frameworks such as the Budapest Convention and co-operation with global cybercrime units have provided Azerbaijan with the tools to

pursue cybercriminals beyond its borders and recover from incidents more efficiently. The implementation of legal mechanisms has been demonstrated to reduce the impunity of attackers and serve as a deterrent, thereby indirectly protecting economic interests. Azerbaijan's experience demonstrates the importance of aligning cybersecurity initiatives with economic policy. By allocating resources to the development of cybersecurity infrastructure, educational initiatives, and effective governance, Azerbaijan is able to foster stability in its GDP and enhance market confidence. The proactive measures implemented in the financial sector, the establishment of training centres, and the introduction of incentives for cybersecurity development all serve to illustrate a model in which economic growth and cybersecurity are inextricably linked. Azerbaijan serves as a case in point, with its rising cybersecurity rankings and sustained growth in its digital services sector, despite a paucity of major incidents. However, the dynamic nature of cyber threats necessitates continuous adaptation. As Azerbaijan's economy becomes more digitised, embracing cloud computing, fintech innovation and Industry 4.0 technologies, the threat landscape will evolve. Future research and policy development should focus on areas such as quantifying the impact of cyber incidents on economic indicators in Azerbaijan, strengthening public-private partnerships in cybersecurity, and exploring cyber insurance markets to mitigate residual risks. In conclusion, Azerbaijan's journey in combating cybercrime illustrates that while a robust legal framework and international co-operation are important foundations, the ultimate goal is economic security. By making cybercrime prevention an economic priority, Azerbaijan is taking commendable steps to secure its digital future. The world practices reviewed in this article – from global cost assessments to collaborative defense strategies – reinforce that no country can afford to treat cybersecurity in isolation from economic policy. The notion of a safe cyberspace has become increasingly intertwined with the notion of a healthy economy. Azerbaijan's ongoing efforts in this regard can serve as a useful case study for other emerging digital economies facing similar cyber threats.

References:

Akhundov, K. (2023). Azerbaijan beefing up defence strategy against cybercrime. Caliber.Az. Available at: https://caliber.az/en/post/azerbaijan-beefing-up-defence-strategy-against-cybercrime

Alazraq, N. (2021). Criminal Liability Determinants of Hacking, Interception & Plagiarism and Ways of Regulation and Deterrence in Arab Legislations in the Digital Age: Analytical comparative study. *Journal of Mass Communication Research*, Vol. 56(3), p. 1041–1080. Available at: https://jsb.journals.ekb.eg/article_150183.html?lang=en

Balajanov, E. (2017). Effectiveness of Cybercrime Law Enforcement in Azerbaijan. [Conference presentation]. Centre for Criminal Justice Studies PGR Conference, University of Leeds. Available at: https://www.researchgate.net/publication/317562309_Effectiveness_of_Cybercrime_Law_Enforcement_in_Azerbaijan

Buçaj, E., & Idrizaj, K. (2024). The need for cybercrime regulation on a global scale by international law and cyber convention. *Multidisciplinary Reviews*, Vol. 8(1), p. 20–24. DOI: https://doi.org/10.31893/multirev.2025024

Codex (2008). Agreement on Co-operation between the CIS Member States in the fight against computer information crimes. Available at: http://docs.cntd.ru/document/902140948

Council of Europe (2003). Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Available at: http://zakon.rada.gov.ua/laws/show/994_687

Council of Europe (2009). Economic Crime Division: The functioning of 24/7 points of contact for cybercrime (discussion paper). Available at: https://rm.coe.int/16802fa3be

Council of Europe (2021). Convention on Cybercrime (ETS No. 185). Available at: https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf

Council of Europe (2025). International co-operation against cybercrime. Available at: https://www.coe.int/en/web/cybercrime/international-co-operation

Dharminder, K., Nilutpal, D., Rumi, D., Monmi, G., Akkas, A., & Upasana, B. (2023). Combating Cybercrime: An Analysis of National and International Legal Mechanisms. Tuijin Jishu. *Journal of Propulsion Technology*, Vol. 44, p. 6–15. Available at: https://www.propulsiontechjournal.com/index.php/journal/article/view/3827

Didkivska, G., & Shevchenko, D. (2023). Basic principles of combating cybercrime: international experience. *Legal Horizons*, Vol. 19, p. 19–23. Available at: https://www.researchgate.net/publication/381905924_Basic_principles_of_combating_cybercrime_international_experience

Donalds, C., & Osei-Bryson, K.-M. (2018). An ontological approach to classifying cybercrimes in an ICT4D context. In J. Steyn, G. Johanson, & J. van Belle (Eds.), ICTs for Inclusive Communities in Developing Societies (pp. 253–267). Springer. DOI: https://doi.org/10.1007/978-3-319-91800-6_17

ENISA (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. (High Representative of the EU for Foreign Affairs and Security Policy report). Available at: http://www.enisa.europa.eu

Europol (2018). Internet Organised Crime Threat Assessment (IOCTA) 2018. Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organisedcrime-threat-assessment-iocta-2018

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability (IMF Working Paper WP/17/185). International Monetary Fund. Available at: https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45183

Li, M., & Stephenson, M. (2024). Investing in the Digital Economy of Azerbaijan (IDEA) – Insight Report. World Economic Forum. Available at: https://www3.weforum.org/docs/WEF_IDEA_Investing_in_the_Digital_Economy_of_Azerbaijan_2024.pdf

NATO CCDCOE (2025). Co-operative Cyber Defence Centre of Excellence (CCDCOE). Available at: https://ccdcoe.org/about-us/

Samedova, Sh. T. (2020). Criminal Law of the Republic of Azerbaijan. Baku: [Monograph]. Available at: https://academy-aba.az/api/books/1721627836620.pdf

Spînu, N. (2020). Azerbaijan Cybersecurity Governance Assessment. Geneva Centre for Security Sector Governance (DCAF). Available at: https://www.dcaf.ch/sites/default/files/publications/documents/AzerbaijanCybersecurityGovernanceAssessment.pdf

United Nations Office on Drugs and Crime (2016). International legal frameworks for combating cybercrime: the UNODC perspective. Available at: https://www.oas.org/juridico/PDFs/cyb9_unodc_Dec16_v1.pdf

United Nations (2022). Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes – Overview of Existing Instruments (A/AC.291/CRP.10). Available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

United Nations (2024). International and regional instruments (Cybercrime Module 3). Available at: https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-3/key-issues/international-and-regional-instruments.html

Received on: 23th of January, 2025
Accepted on: 07th of March, 2025
Published on: 04th of April, 2025