The Role of Cyberattacks in Political and Economic Stability: Transforming National and International Approaches

Submitted: 10 October 2025
Reviewed: 8 January 2026
Revised: 27 February 2026
Accepted: 1 March 2026

Aizhana Myrsalieva[*]
https://orcid.org/0009-0001-4758-8505
Elia Abdrakhmanova[**]
https://orcid.org/0009-0000-1632-7962
Daniyar Suiunduk uulu[***]
https://orcid.org/0009-0008-5250-9825
Maksatbek Moldomyrzaev[****]
https://orcid.org/0009-0001-1849-3013

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v18i2.59089

Abstract

[Purpose] The purpose of the study was to identify the main aspects of threats in the cyber sphere to determine recommendations for improving cyber resilience.

[Methodology/approach/design] The study used materials from the Centre for Strategic and International Studies (CSIS), reports and publications from Arctic Wolf and UpGuard, cyber resilience indices from MixMode, and publications from the Global Organised Crime Index. The research methods were case studies, statistical analysis, and analysis of official documents.

[Findings] The study found that cyber incidents as a phenomenon have been known since at least the early 2000s, but the main increase in activity began after 2015. In addition, the intensity of cybercrime was influenced by international events, such as the 2008 crisis, the coronavirus epidemic in 2020, or the full-scale Russian invasion of Ukraine in 2022. Government structures are among the most common targets of cybercriminals. In this context, cyber warfare, cyber espionage, and hacktivism can be used. It has also been studied that, in the context of the economic consequences of cyber threats, the main target

[*]Postgraduate Student, Head of the Department of Industry Economics, Limited Liability Company "Inmobiles", 720040, 197/1 Tynystanov Str., Bishkek, Kyrgyz Republic. E-mail: myrsalievaaizhana@gmail.com.
[**]Postgraduate Student, Head of OAO Optima Bank, 720044, 95/1 Chingyz Aitmatov Ave., Bishkek, Kyrgyz Republic. E-mail: e-abdrakhmanova@outlook.com.
[***]Postgraduate Student, Head of the Department of Constitutional and Municipal Law, Nazaraliev Medical Centre, 724330, 84 Bolshevik Str., Bishkek, Kyrgyz Republic. E-mail: d_suiundukuulu@hotmail.com.
[****]Postgraduate Student, General Manager of the Department of Political Institutions, Processes and Technologies, Design and Construction Company "Dream Architect", 720017, 195 Bokonbaev Str., Bishkek, Kyrgyz Republic. E-mail: m.moldomyrzaev@outlook.com.

of criminals can be cloud storage, because the volume of data stored in them increases every year. In addition, losses from cybercrimes in 2018 were estimated at 600 billion dollars, and by the mid-2020s they were estimated to have reached approximately 9.2 trillion dollars. The exact number of cyber incidents is extremely difficult to track due to their geographical disparity. In this regard, large companies and corporations are strengthening their cyber resilience, an example of which is the activities of JPMorgan Chase. In the context of individual countries, developed economies are the most resistant to cyber incidents, while in developing countries the situation with cyber resilience is much worse. At the national level, one of the most successful cyber security strategies is the Finnish model. It is also important that the draft resolution "United Nations (UN) Convention against Cybercrime" was approved at the international level. As a result, the international community continues to face threats of cyber incidents, but more and more initiatives are being taken to minimise the risks of cyber threats.
[Practical implications] The findings highlight the need for adaptive cybersecurity strategies, particularly in cloud storage protection and national infrastructure. They support the importance of strengthening cyber resilience in developing countries, adopting best practices from successful models (e.g., Finland), and enhancing international coordination.
[Originality/value] The study provides a longitudinal analysis of cybercrime trends in relation to major global events and links the rise in cyber incidents to geopolitical and economic disruptions.

Keywords: Financial Sector. International Cooperation. National Strategy. Hacktivism. Phishing. Cybersecurity. Political Stability.

INTRODUCTION

In the 21st century, the rapid development of digital technologies has become an integral part of everyday life, as well as a critical factor in the development of political stability and economic security of states. The integration of digital technologies into financial systems and aspects of public administration creates opportunities for rapid progress. However, despite these advantages, digital technologies have also created unprecedented challenges associated with cybersecurity threats that affect both individuals and entire governments, as well as international relations in general. The relevance of the study also lies in both the quantitative and qualitative growth of cyber incidents affecting global markets and social stability (Ahmad et al., 2021; Chigada and Madzinga, 2021).

An additional important aspect in the context of the topic is hacker attacks on government agencies, financial organisations, and critical infrastructure facilities. Hacker attacks on energy systems, the banking sector, or healthcare institutions can undermine security and cause negative consequences for millions of people (Arctic Wolf, 2025; Microsoft, 2022). Ensuring cybersecurity in the context of globalisation and digitalisation, as one of the main drivers of the world economy, is becoming a matter not only of protecting national security at the level

of technical protection, but also of establishing a distinct strategy for managing a modern state (Cavelty and Wenger, 2022; Centre for Strategic and International Studies (CSIS), 2024).

In addition to the above, studying aspects of cybersecurity in the context of political stability is also important due to the role of cyber weapons as an instrument of geopolitical influence. Governments themselves can also use cyberattacks to achieve certain political and economic goals, which leads to the violation of the sovereignty of individual states and creates a context of geopolitical tension on the world stage (Dawood, 2021; Codreanu, 2022). Such activities can include interference in electoral processes, destabilisation of the information space, and undermining trust in government through propaganda. It is in such conditions that the ability of individuals, organisations, or governments to resist cyber threats can have a direct impact on maintaining political and economic stability (Rizzoni et al., 2022; Shandler and Gomez, 2023).

The economy also plays a crucial role in the modern world and is therefore highly susceptible to cyber threats (AYUPOVA and SERALIYEVA, 2015; SASI et al., 2023). In the mid-2020s, global economic processes remain unstable due to the long-term consequences of the coronavirus pandemic, ongoing geopolitical conflicts, and Russia's full-scale invasion of Ukraine in 2022. Cyberattacks pose a serious threat to businesses and corporations. According to forecasts from Statista (2025) and Cybersecurity Ventures (2025), cybercriminals' income may rise to USD 10.5 trillion, in 2026 to USD 11.3 trillion, and in 2027 to USD 12.4 trillion (Increase in the number..., 2024). These forecasts reflect broader trends in the expansion of the digital economy and may be adjusted depending on the pace of artificial intelligence integration on both the defensive and offensive sides of cyberspace. Thus, while governments, corporations, and business entities may be better equipped to counter cyber threats, cybercriminals will likewise gain new tools to advance their activities (Check Point Research, 2025; Zwilling et al., 2022).

What is also important is that the digital transformation of the economy significantly increases the dependence of government structures on the reliability of cyber infrastructure. The effectiveness of cyber defence institutions largely depends on the degree of public trust in governmental bodies (AKSHATAEVA et al., 2016). In the event of failures in the state cybersecurity system, there are risks not only of losing economic resources but also of forfeiting strategic advantages on the global stage (Law of the Kyrgyz Republic No. 121, 2024; Resolution of the Kyrgyz Republic, 2023). Given this, research into cybersecurity in the context of political and economic stability is essential for understanding modern challenges and for developing strategies that enable international actors

to maintain resilience and economic competitiveness in a rapidly evolving digital environment.

In the work of A.A. Alikhanov and A.T. Gyyazov (2023), aspects of ensuring economic security at the state level in the context of digitalisation were studied. The authors pointed out that cybersecurity includes, in particular, the reliability of storing digital information – that is, preventing any loss of data due to failures in telecommunications infrastructure – as well as protection against theft, hacking, or destruction. Ensuring cybersecurity at the national level involves providing access to digital means of storing information for businesses and the population (BAIMUHAMEDOV et al., 2019; PETRAKOV et al., 2019). In another study, A.A. Alikhanov (2023) noted that in the context of digitalisation, ensuring cybersecurity is critically important for both the population and business structures. Higher cybersecurity levels enable more transactions between enterprises in the form of digital payments, and accordingly, increase Internet use for interaction between the population and businesses (KARASHEVA et al., 2024; BARLYBAYEV et al., 2024).

M.D. Cavelty and A. Wenger (2022) wrote that the external focus of cyber threats is the growing willingness of criminals to exploit the weaknesses inherent in societies without restraint or hesitation. The internal focus is on the vulnerabilities inherent in computer systems. As a result, cybersecurity has become a type of security that refers to offensive and defensive actions by both state and non-state actors in cyberspace, which serves as a mechanism for achieving political goals.

The study by R. Shandler and M.A. Gomez (2023) examined the ways cyberattacks undermine public trust in government. The authors highlighted that certain qualities of cyberattacks – such as their stealthiness, unpredictability, and potential for widespread disruption – exacerbate public concern. By exploiting vulnerabilities in government systems and creating uncertainty about the state's ability to protect sensitive information, cyberattacks significantly reduce citizens' confidence in government institutions. Shandler and Gomez (2023) emphasise that it is not only the direct damage caused by attacks that matters, but also the perceived incapacity of authorities to prevent or respond effectively, which fosters skepticism and fear among the population. Y. Dawood (2021) studied the approaches of the Canadian electoral ecosystem to disinformation and cyberthreats. The strategy consisted of preventing foreign individuals and groups from influencing elections, reducing disinformation in the information discourse, and strengthening Canada's cybersecurity system. The study by O. Gulyas and G. Kiss (2023) described specific actions to protect global financial systems, namely:

intensifying information sharing, encrypting data storage, and harmonising regulations and jurisdictions to combat international crime.

The author O. Kayode-Ajala (2023) identified the main challenges that developing countries face in building cyber resilience, namely institutional resilience, regulatory mechanisms, financial constraints, educational imperatives, and public-private sector cooperation. M.D. Cavelty et al. (2023) proposed three ways to improve cyber resilience, namely interdisciplinary research, and public debate in the decision-making process.

Based on the above, the purpose of the study was to identify the main threats in the cyber sphere to understand the landscape of minimising their risks. The objectives of the study were to analyse threats in the political and economic spheres, as well as to determine the importance of forming national and international strategies to counteract cyber threats.

MATERIALS AND METHODS

The paper analyses materials in the context of threats to government agencies: CSIS (2024) on cyber incidents, Check Point Research (2025) on cyberattacks on government agencies, and ESET Research (2023). Microsoft reports (2022) on malware and Radio Free Europe (RFE) (2022) data on politically motivated attacks are considered. Arctic Wolf (2025) materials on key attacks on government agencies and information from UpGuard (2024) are also analysed.

Threats to the financial sector: the views of the President of International Business Machines (IBM) (Morgan, 2015) on cybercrime (Morgan, 2015) and Cybersecurity Ventures (2025) forecasts on the growth of threats are studied. UpGuard (2025) and World Economic Forum (WEF) (2024) reports on economic losses and McAfee (2018) research are considered. The International Monetary Fund (IMF) (2024) reports and the JPMorgan Chase case study (Financial Times, 2024) were also examined.

Cybercrime in developing countries: the Global Organized Crime Index (2025) data on Albania and Kyrgyzstan were analysed, as well as the official statistics of Kyrgyzstan (National Statistical Committee…, 2024; Economist.kg, 2024).

International cyber resilience initiatives: the MixMode (2024) data on the cybersecurity of countries, the North Atlantic Treaty Organisation (NATO) (2023) and Euronews (2023) materials on Finland's accession to NATO were considered. The Finnish cybersecurity strategy was also considered (Ministry for Foreign…, 2023; Paananen et al., 2024). The cyber defence strategies of Kyrgyzstan (Cybersecurity Strategy…, 2019; Resolution of the Kyrgyz

Republic…, 2023; Law of the Kyrgyz Republic No. 121 "On Cybersecurity of the Kyrgyz Republic", 2024) and the adopted UN Convention against Cybercrime (2024) were also studied.

Disinformation and political consequences of cyberattacks: the Democratic National Committee (DNC) data leak (Reuters, 2016; CNN, 2016), the influence of social networks on disinformation (International Policy Digest, 2022), and the political consequences of cyberattacks (Parliamentary Assembly…, 2024) were analysed.

Statistical information: data on global economic growth from the World Bank Group (2024, 2025), data from Gartner (2023), and information from Statista (2025) and Tempo (2024) were also used. The Data Breach Investigations Report (2011, 2015, 2020) was also reviewed. The History resource (2023) was also used.

The work analysed reports from official government and international agencies using content analysis. The main selection criteria were the relevance of the information or the use of the latest known data. The work also used a case study to analyse specific cases of the impact of cyberattacks on political stability. Statistical analysis was used to compare the growth of global gross domestic product (GDP) and cybersecurity spending. Statistical analysis was also important for determining global financial losses from cyberattacks. The analysed countries were Finland, Ukraine, Iran, Great Britain, Kyrgyzstan, and Albania.

The recommendations were formed based on the analysis of international strategies. In particular, the study of the Finnish cyber defence model made it possible to highlight the main aspects of a successful state strategy. In addition, the analysis of cyberattacks on government agencies also made it possible to highlight the need to implement additional security measures. The recommendations described were also linked to the rapidly developing capabilities of artificial intelligence.

RESULTS

The Impact of Cyberattacks on Political Stability

In 1962, CSIS was founded at Georgetown University in Washington, DC, with the goal of identifying ways for the United States to develop and survive as a nation. In the 21st century, this organisation has become a bipartisan and non-profit institution focused on policy research and advancing ideas to address the world's most critical problems. Since 2006, the organisation has been reporting the most significant cyber incidents, including cyberattacks on government agencies, defence, and other high-tech companies. Over time, the number of such cyberattacks has continued to grow (Figure 1). The study by O.I. Falowo et al. (2022) also utilised consolidated data on cyber incidents from CSIS. The authors

emphasised that the findings from CSIS are cross-verified by data from the Data Breach Investigations Reports (2011, 2015, 2020), which demonstrates the reliability of the information.

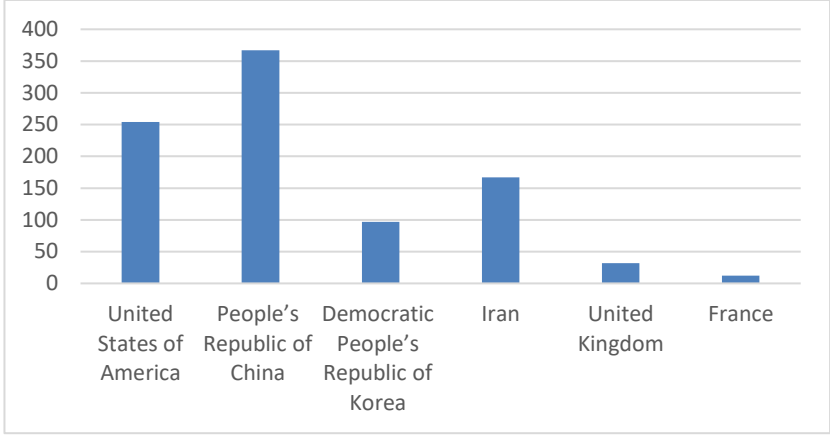

Figure 1 – Number of significant cyber-attacks and their connection with international actors.

Source: created by the authors based on Centre for Strategic and International Studies (2024).

In this context, the term "connection" does not imply definitive attribution of responsibility but rather represents a combination of two factors: (1) the frequency with which specific international actors are mentioned in reports of cyber incidents and (2) inferred responsibility based on publicly available evidence, such as malware signatures, attack patterns, and geopolitical context. Essentially, Figure 1 shows which countries or actors are most frequently associated with significant cyberattacks, highlighting patterns of state-sponsored or politically motivated cyber activity, without asserting absolute proof of culpability.

Based on the information received from CSIS, critical cyberattacks that resulted in losses of more than USD 1 million, disruption of government agencies, defence companies, or other important technology systems occurred in 2006-2015, but their growth rate was not high. However, since around 2015, their number has increased sharply, reaching a peak in 2020 – at the height of the coronavirus pandemic, when a significant share of businesses, government and non-governmental organisations, as well as other actors in international relations, moved their activities online. Figure 1 illustrates the international aspect of these incidents by indicating the states or actors frequently referenced in connection with cyberattacks, rather than offering legally enforceable attributions.

With the decline of the epidemic, the number of cyber incidents could have decreased, but in 2022, alongside Russia's full-scale invasion of Ukraine, the geopolitical situation deteriorated. The polarisation of international relations, with alignments either closer to the United States or to the People's Republic of China (PRC), became more pronounced. The most frequently mentioned subjects of international relations in the context of cyberattacks include the Democratic People's Republic of Korea (DPRK), China, the USA, Iran, the Republic of Korea, Ukraine, and the United Kingdom. This pattern of mentions constitutes the "connection" visualised in Figure 1, indicating which actors are recurrently implicated in cyber incidents through analysis of open-source intelligence and reporting, rather than asserting conclusive attribution.

In the work of researchers P.H. Meland et al. (2021), the characteristics of cybersecurity incidents in the maritime transport sector were examined. According to the authors, the increase in cyber activity in this sector began in 2015. Similarly, the information presented in Figure 1 supports this observation. Moreover, as the number of cyberattacks increases, their sophistication also evolves, suggesting the likely absence of a single cause that could be definitively eliminated.

Cyberattacks against government institutions are widespread for several reasons (Check Point Research, 2025). Primarily, these institutions become targets of various hacker and criminal groups driven by diverse motivations. This may include cyberwarfare aimed at undermining a state's ability to wage conventional war, as well as causing harm to the government and its citizens. According to C. Ashraf (2021), for over 30 years, scholars have proposed varying definitions of cyberwarfare, yet consensus remains elusive. The main points of contention concern the denial of cyberwarfare's existence or whether it constitutes an imminent threat to humanity. Another form of activity is cyber espionage, where states seek strategically valuable information from rival governments. In such cases, cyber groups with state sponsorship may carry out operations to steal confidential information. Cyber espionage dates back to the Cold War and, in the 21st century, has become "commonplace" in interstate relations (History, 2023). However, cyber espionage can also result in serious tensions if such operations are publicly exposed (DEVANNY et al., 2021). A further example is hacktivism. These actors are often motivated by ideological or political visions for reforming the political system within a given state. Their actions aim to promote their beliefs through cyberattacks. Hacktivist groups often employ methods such as Structured Query Language (SQL) injection, web server misconfiguration, Distributed Denial of Service (DDoS) attacks, and hacking of social media accounts (CHNG et al., 2022). A case in point is the series of Russian cyberattacks on Ukrainian organisations before and during the full-scale invasion in 2022 (ESET Research,

2023). Such cyberattacks may be premeditated. For example, on 16 January 2022, Microsoft's social network account on platform X indicated that the company had identified a unique and destructive malware exploited by a group called DEV-0586 to target Ukrainian organisations. An example of politically motivated hacktivism – specifically, an attempt to challenge an existing ideological system – was the attack by a dissident hacker group during live broadcasts on several Iranian state television channels (Radio Free Europe, 2022). The hackers declared that the Iranian regime "will no longer silence us, and government palaces will be opened so that people can punish them".

According to Arctic Wolf (2025), an organisation that monitors, detects, and responds to cyber threats, government agencies were among the top five industries subjected to ransomware or business email compromise cyberattacks in 2023. Government organisations are particularly profitable targets for hackers due to several factors: they often rely on technically outdated management systems and software; there is a lack of funding, resources, and expertise to strengthen their cybersecurity posture; the sheer number of government agencies is very high, making them attractive targets; and many of these agencies operate within the same network, which facilitates the spread of ransomware viruses across multiple institutions simultaneously. The study by J. Chigada and R. Madzinga (2021) also noted that healthcare organisations are especially vulnerable to cyber threats, as attackers are aware that these institutions collect and store sensitive data such as bank card details and identification information. However, there are a number of measures that can be implemented within government agencies to enhance their resilience to cybercrime. Comprehensive staff training should be introduced, particularly with a focus on phishing threats. This type of cybercrime forms the basis of social engineering tactics employed by cybercriminals targeting government agencies, where employees often rely heavily on email and may lack awareness of the associated risks. Specific actions include phishing simulations and structured training programmes, which can simultaneously protect government personnel and bolster information security at both governmental and citizen levels. Researchers F. Rizzoni et al. (2022) also highlighted the importance of phishing simulations for training staff within the healthcare sector. However, the authors cautioned that such training initiatives could impose an additional burden on already fatigued employees, potentially impacting the working environment negatively. To recover the information environment in the event of a cyber incident, it is essential to perform regular file backups (SASI and SWARNA JYOTHI, 2019; DAHAN et al., 2025). This practice greatly facilitates the restoration of information systems, databases, and other mechanisms of government agencies in the aftermath of a cyberattack. Additionally, implementing an identity and access management (IAM) system may prove

beneficial. As government employees access confidential data on a daily basis, 24-hour monitoring systems can prevent data breaches before hackers begin their activities.

Cyberattacks have numerous characteristics that directly erode public confidence (ZHUMALIEV, 2022; REXHEPI et al., 2023). They frequently focus on symbols of power, such as governmental institutions, and capitalise on apparent weaknesses to foster ideas of ineptitude or carelessness. Attacks can be extensively broadcast, regardless of their success or failure, instilling fear and worry even in the absence of physical harm. The employment of disinformation, leaks, and social media manipulation exacerbates confusion and polarisation among the populace (ABDYGALYM et al., 2025; ZHANZHUMENOV et al., 2022). Furthermore, cyberattacks are frequently persistent, recurrent, and occasionally clandestine, instilling a perpetual sense of vulnerability among citizens. Attacks may be intentionally scheduled to align with elections, crises, or public events, so amplifying their psychological and cultural effects.

According to a briefing note by a member of the Parliamentary Assembly of the Mediterranean (2024), autocratic states are exploiting the structural vulnerabilities of democratic systems through disinformation and cyberattacks. The ultimate aim is to weaken democratic institutions, undermine internal cohesion, and shift public opinion. These information operations frequently exploit social networks, whose algorithms favour the most polarising content. Consequently, marketing mechanisms on social platforms contribute to the spread of seemingly credible yet fundamentally false narratives, resulting in declining societal commitment to democratic values. This situation highlights the need for regulation of the information sphere, which, however, may come into conflict with core principles such as freedom of speech, press, and expression. In the work of C.M. Codreanu (2022), it was also noted that autocratic governments have begun using digital tools to retain power and exert control over their own populations, thereby creating a necessity to address the phenomenon of "digital authoritarianism".

Cyberattacks, regardless of their success, can influence public sentiment. A study by the organisation Political Violence at a Glance (SHANDLER et al., 2022) examined an example from the summer of 2022, when the Federal Bureau of Investigation (FBI) announced that it had prevented a cyberattack on a government agency. Although the attack did not result in visible damage, it posed a hidden threat, such as undermining social cohesion and reducing trust in the government. The organisation conducted an experiment involving 10,000 respondents from the United States, the United Kingdom, Israel, and Germany. In Germany, respondents were surveyed following a purported "failed" virus attack on a government agency, where authorities had announced the successful

neutralisation of the threat. Nevertheless, the findings revealed a decrease in public trust in the government, as the emphasis in official statements on the physical consequences of the attack provoked deep anxiety among respondents regarding the authorities' capacity to protect them. Overall, the organisation's experiment demonstrated that short-term financial or network damage is not the primary factor influencing societal pressure; rather, the cumulative effect of undermining public trust constitutes a significant component of such cyberattacks.

In addition to the above, manipulation via social media aimed at dividing society is another important aspect. This phenomenon is influenced by recommendation algorithms on such platforms. According to International Policy Digest (2022), fake news spreads six times faster than verified news and is "reposted" 70% more frequently. Furthermore, as the same publication noted, U.S. citizens with differing views on domestic unrest were exposed to curated newsfeeds that reinforced their political beliefs.

In contrast to conventional propaganda or mass media manipulation, which typically depends on centrally generated content disseminated through established routes, social media algorithms dynamically tailor information for individual users. This generates "filter bubbles" and enhances content according to engagement instead of factual correctness, leading to increased polarisation and micro-targeted impact. This mechanism is analytically different in the cyber environment due to its scalability, automation, and utilisation of platform-specific feedback loops, resulting in a more rapid, pervasive, and elusive dissemination of disinformation compared to traditional media efforts. Accordingly, malicious cyberattacks are not the sole method of manipulating public opinion – managing social media algorithms directly shapes the information environment, producing significant societal effects that traditional propaganda alone cannot achieve.

A notable example of the impact of cyberattacks on political stability is the leak of Democratic National Committee (DNC) emails in the United States (CNN, 2016). The leaked emails revealed intra-party bias among committee members, which sparked public controversy and led to the resignation of several officials. According to former Director of the Central Intelligence Agency (CIA), M. Hayden (Reuters, 2016), these manipulations were the work of Russian intelligence services, which deliberately sought to destabilise the geopolitical situation in the aftermath of the commencement of military aggression against Ukraine.

Thus, the study of the impact of cyberattacks on political stability demonstrates that cyber threats extend far beyond technical concerns; rather, they represent a powerful tool of geopolitical influence, social destabilisation, and the undermining of trust in democratic institutions. Some of the primary actors behind cyber incidents are autocratic regimes, which – through the rapid mobilisation of

resources – can effectively exploit the core values and vulnerabilities of democratic systems. This is made possible through the use of social media, disinformation, and technological hacking to generate public distrust in democratic processes and foster the polarisation of opinions within society. In particular, cyberattacks targeting government agencies may serve a strategic purpose: to weaken a state's capacity to conduct military operations, address social issues, or provide critical information and services to the population. The examples of such hacker activity referenced earlier in the text underscore that, since the late 2010s and especially during the global crises of the early 2020s, cyberattacks have become a significant instrument in geopolitical conflicts. Simultaneously, underfunding and technological obsolescence within government institutions contribute to a growing environment for cybercrime and elevate the risk of confidential information leaks – highlighting the urgent need for systematic and strategically coordinated efforts in both personnel training and technical modernization.

Economic Impact of Cyberattacks

Considering the above, the most rapid growth of cybercrime has been noticeable since 2015. It was in 2015 that IBM Chairman, President, and CEO G. Rometty pointed out that data is the phenomenon of our time (Morgan, 2015). Data is a new global resource and the basis of competitive advantage that can transform any profession or industry. The above statement by the senior IBM official was also noted in the work of A. Javaid (2023). Accordingly, cybercrime is the greatest threat to any profession, industry, or company in the world. Additionally, according to Cybersecurity Ventures (2025), the total amount of data in cloud storage – including public clouds of companies (e.g., Microsoft, Apple, Google, Meta), government clouds, and private clouds of large and medium-sized corporations – will reach 100 zettabytes (a unit of measurement equal to 2^{70} standard bytes) in 2025, or 50% of the world's total data, compared to 25% in 2015. This volume of data is of particular interest to cybercriminals. Furthermore, cybercriminals do not necessarily require advanced technical expertise to carry out attacks that can destabilise the economy (UpGuard, 2025). A significant number of malicious software tools are purchased by attackers via the Dark Web, including Ransomware-as-a-Service (UpGuard, 2024), which are sometimes even sold with a "quality mark", access to technical support, and, in the event of malfunction, a refund policy. In the context of cloud storage, researchers W. Ahmad et al. (2021) noted that inadequate data protection may lead to an increase in cybercrime, both against individual users of large online platforms and the platforms themselves – such as Google, Amazon, and Microsoft – as some of the most prominent cloud storage providers.

According to the Global Cybersecurity Outlook from the World Economic Forum (2024), the cybersecurity sector in 2022 was expanding at twice the rate of the global economy. By 2023, this figure had increased to four times the rate of growth of the global economy as a whole (Figure 2).

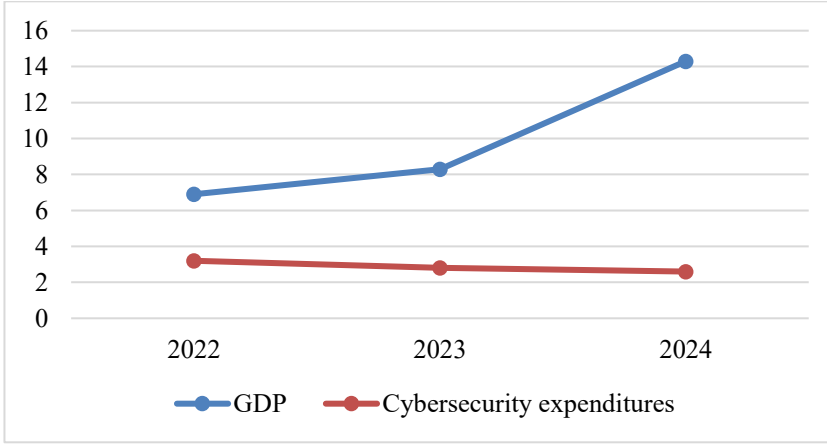

Figure 2 – Cybersecurity GDP and spending growth worldwide (%).

Source: created by the authors based on Gartner (2023); World Bank Group (2024, 2025)

This means that investments by organisations and corporations in cyber resilience are increasing, although innovation can lead to uneven development. According to information from UpGuard, the income of cybercriminals can be imagined by comparison with the revenues of Microsoft. This company, as the world's largest software developer and one of the richest firms overall, reported revenue of USD 200 billion in 2022, while the figures associated with cybercriminal activity may be up to 50 times higher than Microsoft's revenue. In addition, V. Tzavara and S. Vassiliadis (2024) noted that investing in the development of cyber resilience is equivalent to investing in the long-term "survival" of organisations. A joint report by McAfee and CSIS (2018) indicated that approximately USD 600 billion, or about 1% of global GDP, is lost annually due to the actions of cybercriminals, whereas earlier estimates put this figure at only USD 445 billion.

Considering that the number of cybercrimes between 2018 and 2023 continued to grow, it cannot be directly inferred from Figure 2, which presents cybersecurity expenditures rather than crime counts. Therefore, cybercriminals continue to derive enormous profits and cause significant economic harm to individual companies, corporations, and entire governments. For example,

estimated damage from cybercrime, according to Statista (2025), is projected to reach USD 15.6 trillion in 2029, while in the mid-2020s it was estimated at approximately USD 9.2 trillion. The study by L. Kovács and E. Terták (2024) indicated that the intensification of cybercrime is closely linked to global events. For instance, during the 2008 financial crisis, economic losses from cybercrime rose by 115%, and in 2020, during the pandemic, the number of victims increased by 69% compared to 2019. Furthermore, in 2022, losses from cybercrime grew by nearly 30% compared to 2021.

In April 2024, the IMF published its report The Last Mile: Financial Vulnerability and Risks, highlighting that the financial system is particularly exposed to risk. This vulnerability stems from the fact that financial institutions process large volumes of client data, information, and transactions, making them attractive targets for cybercriminals seeking financial gain or attempting to disrupt economic systems. Researchers B.T. Familoni and P.O. Shoetan (2024) have also written that the financial sector is a primary target for cybercriminals, due to its storage of vast amounts of confidential data. Simultaneously, the number of cyber incidents and the scale of financial losses in the financial sector constitute one of the largest shares of overall cybercriminal activity (Figure 3).

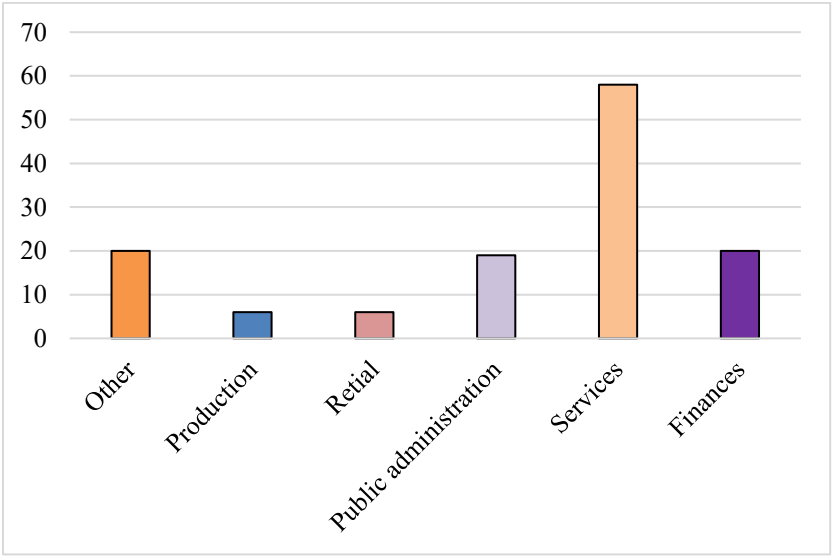

Figure 3 – Number of cyber incidents by sector 2004-2023 (thousands).

Note: The most recent International Monetary Fund financial stability reports available at the time of the study do not include data for the latest reporting year.
Source: created by the authors based on International Monetary Fund (2024).

In the financial sector, up to half of all cyber incidents occur in banks. Large banks are often targeted by cybercriminals due to their higher profits, despite having more sophisticated cybersecurity measures (IMF, 2024). In addition to banks, M.N.U. Milon et al. (2024) identified stock exchanges and international financial transactions as targets for cybercriminals. Financial companies worldwide, although unnamed in the report (IMF, 2024), have reported losses exceeding $12 billion since 2004. Financial institutions in many advanced economies, such as the United States, are the most vulnerable to cyber incidents. In contrast, countries with developing economies are less susceptible to such incidents. Developed economies include Switzerland, Germany, Australia, Denmark, Finland, and the United States, while developing economies include Albania, Mexico, Brazil, Moldova, Indonesia, and others (Tempo, 2024).

For instance, in January 2024, a top executive of one of the largest US investment banks, M. Erdoes, spoke at the World Economic Forum in Davos (Financial Times, 2024). She stated that cybercriminals are becoming more intelligent, cunning, and malicious, which is why JPMorgan Chase (Financial Times, 2024) is increasingly affected by waves of cyberattacks. She also noted that the bank invests approximately $15 billion annually in developing cybersecurity technologies and employs 62,000 technical specialists dedicated to combating cybercrime. Furthermore, she reported that the bank faced 45 billion hacking attempts per day, although this figure was later revised. The study by Y. Liu (2024) also provided additional examples of cybersecurity initiatives at JPMorgan, including investment in firewall upgrades, intrusion detection systems, and data encryption technologies. The bank also introduced a stricter monitoring system for effective incident response and enhanced employee training to improve the identification of cyberattacks.

As mentioned earlier, developing countries are generally less exposed to economic cybercrime. However, O.O. Oyadey et al. (2024) observed that the Asia-Pacific region has become a cybercrime target due to its economic potential and poor cyber resilience. In contrast, developing countries may also serve as sources of cyber threats. According to the Global Organised Crime Index (2025), Albania is the country of origin for a significant share of cybercrime in Europe, committed by both local and foreign actors, accounting for more than 10% of cyberattacks in the region. Despite having relevant legislation, cyber fraud in Albania's financial sector continues to grow, particularly due to cryptocurrency trading. This activity is controlled by organised crime groups, and the financial fraud itself poses a serious threat to Albania's national security and the broader economic stability of Europe. Researcher M. McBride (2024) similarly noted that cybercrime and other criminal activities are integrated into Albania's illicit

economy, which explains the country's Global Organised Crime Index score of 5.17 out of 10 (2023b). In another developing country, Kyrgyzstan, the situation differs. Cybercrime is only partially prevalent, with the main threats being ransomware attacks against individuals, corporations, or the public sector, all of which may endanger national security. Kyrgyzstan is also considered an attractive location for crypto hackers who exploit others' computers for cryptocurrency mining. However, the overall impact of cybercrime remains limited according to the Global Organised Crime Index (2025), owing to Kyrgyzstan's low Internet penetration. S. Chen et al. (2023) indicated that relatively few cybercrime-related Internet Protocol (IP) addresses are located in southern Central Asia, and that cybercrime prevalence is directly linked to regional levels of socio-economic development. Given Kyrgyzstan's modest Internet coverage, the country is likely to be of only moderate interest to cybercriminals.

At the time of data collection in early 2025, the official website of the National Statistical Committee of the Kyrgyz Republic does not contain information on the number of offences resulting from the actions of cybercriminals (National Statistical Committee…, 2024). Certain trends can be identified based on statements by official and authorised representatives of Kyrgyzstan. For example, in March 2024, the Head of the Department of the Main Criminal Investigation Department of the Ministry of Internal Affairs for Cybercrime in Kyrgyzstan, R. Sharshenbiev, noted (Economist.kg, 2024) that the number of cybercrimes has significantly increased in recent years. The methods used by cybercriminals include email-based fraud, theft of digital identities and payment data, the theft and subsequent sale of corporate data, and cyber blackmail. It was also reported that between 16 February and 5 March, 1,030 complaints were registered in the city of Bishkek, with the total damages amounting to approximately 43 million soms. Additionally, in July 2024, the Head of the Department for Operational and Technical Support and Monitoring of Social Networks under the Ministry of Internal Affairs of Kyrgyzstan, S. Alseitov, stated that the number of cybercrimes had increased compared to 2023 (PETCHENKO, 2024). However, official statistics on the number of such fraud cases in Kyrgyzstan remain classified.

The financial sector, being one of the most dependent on digital infrastructure, is particularly vulnerable to cyberattacks. Large banks lose billions of dollars annually, despite significant investments in cybersecurity. At the same time, financial institutions in developed countries are increasingly exposed due to the high volume of transactions and data processing, while developing countries are more often the source of threats rather than their primary targets. Cyberattacks on economic systems result in considerable losses. In 2018, the economic damage caused by cyberattacks was estimated at USD 600 billion, and this figure

continued to rise to USD 9.2 trillion by the mid-2020s, reflecting the sustained growth in the number and scale of incidents throughout the decade. Effectively combating cybercrime requires technological innovation, global cooperation, and improved cyber literacy. However, the pace of cyber threats continues to outstrip the ability of economic systems to adapt, posing an ever-increasing risk to the global economy.

The Role of Public Policy and International Initiatives in Ensuring Cybersecurity

For governments in the 21st century, one of the most important tasks is to ensure cybersecurity, given the serious consequences of cyberattacks, which include financial losses, reputational harm, and disruption to the operations of government bodies and other critical structures essential to the functioning of both public and private sectors. Researcher I. Tasheva (2021) noted that the most significant intensification of cyber threats to the public sector was observed during the coronavirus pandemic of 2020. According to statistics from MixMode (2024), the most cyber-resilient countries are those of Western civilisation (Table 1).

Rank	Country	National Cyber Security Index	Cyber Threat Exposure Index	Global Cybersecurity Index	Cyber Resilience Index	Cybersecurity Final Assessment
1	Finland	86	89	96	94	93
2	Norway	68	87	97	94	93
3	Denmark	84	88	93	96	92
4	Australia	66	87	97	86	90
5	United Kingdom	90	79	100	90	90
65	Kyrgyzstan	38	31	50	76	52
66	Ecuador	53	35	26	74	45
67	Algeria	34	28	34	68	43
68	Venezuela	29	19	27	80	42
69	Honduras	22	40	2	82	41
70	Bolivia	31	22	16	77	38

Table 1 – Countries with the highest and lowest levels of cyber threat risk.

Source: created by the authors based on MixMode (2024)

Overall findings from MixMode (2024) show a high level of cybersecurity in Finland, Denmark and Norway, indicating a robust cybersecurity infrastructure and the ability to respond quickly to cyberthreat risks. Finland exhibits the most holistic approach among these nations, amalgamating innovation, vital

infrastructure protection, and international collaboration into a unified plan. This comprehensive methodology has demonstrated efficacy in swiftly addressing emerging cyber threats and sustaining high resilience in governmental and societal systems. In contrast, Bolivia, Honduras and Venezuela face serious cybersecurity challenges. At the same time, cyberthreats in Kyrgyzstan are evolving, requiring comprehensive measures to further develop cyberthreat protection mechanisms. Countries such as Poland, Turkey, and Portugal are not included in Table 1; however, research by M. Zwilling et al. (2022) indicates that these nations exhibit average cyberresilience levels. [Added clarification to justify the mention of these countries.] In their study of cybersecurity knowledge and behaviour in Poland, Turkey, Israel, and Slovenia, the authors concluded that the populations are generally aware of cyberthreats but implement only minimal protective measures, suggesting a moderate national cyber resilience in practice.

A historic shift that has further increased the Finnish government's focus on cybersecurity was Russia's full-scale invasion of Ukraine in 2022. The Finnish plan, tailored to address direct geopolitical concerns and facilitate swift, coordinated responses, underscores the significance of situational awareness, intersectoral collaboration, and continuous resource allocation. These attributes render it an exemplary example for guiding the formulation of suggestions for other nations and organisations aiming to enhance cyber resilience. This is due to the fact that Finland shares a more than 1,000 km border with Russia in the east of the country. Accordingly, after Finland abandoned its neutrality policy and joined NATO (2023), the Russian government made statements about taking "countermeasures" to address security threats following Finland's NATO membership (Euronews, 2023). Given that the Russian government is already waging the largest war in Europe since the Second World War, its aggression against Finland may focus specifically on cyber threats. According to the Ministry for Foreign Affairs of Finland (2023), the goal of Finland's national cybersecurity strategy is to respond as quickly as possible to cyber threats, strengthen the security of society, and ensure the functioning of cyberspace under all conditions (PAANANEN et al., 2024). The cyber threat aspect of the Russian government has also been described in the work of H. Çifci (2024).

The updated strategy in Finland covers the period from 2024 to 2035 and consists of four pillars (PAANANEN et al., 2024). The first is the development of competence, technology, research, development and innovation. The strategic goals are to increase competence through education, gain an advantage through the integration of security in software and services, achieve self-sufficiency in critical cryptographic technologies, and fully utilise the benefits of cooperation within the EU and NATO. The goals of the second pillar are to support the cyber resilience of infrastructures critical to the functioning of society, prepare

authorities and individuals for cyber threats, promote the Finnish cybersecurity model as a separate export product, support comprehensive awareness of cyber threats, and ensure long-term resourcing of all entities in public administration. The objectives of the third pillar are active cooperation and support of partner countries in the field of cybersecurity, close cooperation between the public and private sectors, and unimpeded exchange of information between government agencies. The objectives of the fourth pillar are that responses and countermeasures to cyber incidents should be based on situational awareness and aimed at combating organised and serious cybercrime.

Cybersecurity strategies are also adopted in developing countries, as they are also susceptible to cyber incidents. In 2019, Kyrgyzstan adopted the Cybersecurity Strategy for 2019-2023 (2019). The goal of the Strategy was to form a national cybersecurity policy system to ensure the security of all citizens of Kyrgyzstan, businesses, and the government. The objectives of the strategy were: forming the basis for a unified cybersecurity system in the country; establishing a unified terminology framework in the field of cybersecurity; reducing the number of cyber incidents through the development of warning, response, and management systems for computer incidents; forming a regulatory framework in the field of cybersecurity; modernising information protection standards; and increasing the level of awareness and competence of human resources in the field of cybersecurity. As part of the implementation of this Strategy, many results were achieved. In particular, in 2020, the Coordination Centre for Cybersecurity of the State National Security Committee of the Kyrgyz Republic was established (Resolution of the Kyrgyz Republic…, 2023). Its main objectives at the time of analysis are to implement cybersecurity policy, prevent and suppress computer attacks, coordinate the actions of government agencies, make proposals to improve legislation, and ensure the fulfilment of obligations assumed by the Government of Kyrgyzstan under international treaties in the field of cybersecurity. In 2021, the Agency for the Protection of Personal Data under the Cabinet of Ministers of the Kyrgyz Republic was also established (State Personal Data…, 2025). In July 2024, Law of the Kyrgyz Republic No. 121 "On Cybersecurity of the Kyrgyz Republic" (2024) was adopted, defining the legal basis for a unified cybersecurity system in matters of protecting individuals, society, and the state by supporting the digital resilience and information infrastructure of the state. In addition to the above, the curriculum for computer science in grades 5-9 was modernised. Subjects such as "cybersecurity", "digital literacy", "computer hygiene", "programming", and "system administration" were introduced (Strategy for the protection…, 2024).

The fight against cybercrime is a task that cannot be carried out alone. At the end of December 2024, the UN adopted a historic Convention against

Cybercrime by consensus vote after five years of negotiations. As stated in the publication on the UN website (2024), prior to its adoption, there had been no single universally agreed convention on cybercrime. The new strategy will allow for the most effective and rapid coordinated response, making both the digital and physical worlds safer (UN, 2024). The strategy focuses on access to electronic evidence, its exchange, and assistance in investigations and prosecutions. This is important given that the problem of cybercrime is the centralisation of data and networks, which means that potential evidence of the guilt of certain cybercrime actors may be located under the jurisdiction of different states. Accordingly, states parties to the convention will be able to more effectively and quickly obtain the information they need and provide mutual assistance. In addition, the convention establishes more effective tools for protecting children in the Internet space. The strategy also contains clauses that urgently call on member states to develop comprehensive strategies for preventing and combating cybercrime. International cooperation allows countries to pool their resources, experience and efforts in the fight against cybercrime, increases their resilience, and forms a "united front" to combat the evolving threat landscape (WIDODO et al., 2024).

International cybersecurity initiatives and government programmes play a key role in minimising the risks of cyberattacks and increasing global cyber resilience (SMAILOV et al., 2025; BARLYBAYEV and TURGINBAYEVA, 2025). The Finnish model was selected for the formulation of the recommendations due to its demonstration of a successful, holistic strategy that integrates swift threat response, advancements in cybersecurity technologies, safeguarding of key infrastructure, and efficient international collaboration. The clear structure, quantifiable objectives, and adaptability to evolving challenges offer a pragmatic foundation for other nations and organisations to replicate. By adhering to this paradigm, policymakers may guarantee that recommendations are based on a validated strategy that harmonises technological, organisational, and societal dimensions of cybersecurity.

Kyrgyzstan, although making progress in developing cyber resilience, still needs to be modernised. The previously introduced strategy for 2019-2023 created the basis for a systemic approach to protecting the digital space, but challenges remain relevant. The Law of the Kyrgyz Republic No. 121 "On Cybersecurity of the Kyrgyz Republic", adopted in 2024, and the inclusion of cybersecurity in educational programmes are important steps to improve the situation. The adoption of the global Convention against Cybercrime in 2024 was a historic moment in the fight against cyber threats. Coordination between countries can now be faster and more effective, which will contribute to the security of both the digital and physical worlds.

CONCLUSIONS

The results of the study demonstrated that cyberattacks are a serious tool for geopolitical influence, the destabilisation of individual communities, and even the undermining of trust in democratic institutions by authoritarian actors in international relations. Along with the development of information technology, cybercrime has also evolved, as evidenced by the increase in cyber incidents since the early 2000s. In addition, cyber technologies tend to be used in international conflicts, as was the case before and during Russia's full-scale invasion of Ukraine. Consequently, autocratic regimes can use cyberattacks to disinform the population via social networks. Cyberattacks can also affect the ability of the public sector to effectively perform its critical functions. This necessitates a strategic strengthening of cyber defence, whether through investment in more advanced technical resources or in personnel training and the systematic updating of information hygiene aspects.

It was also noted that cyberattacks have a serious impact on economic stability, causing multi-million-dollar damage to companies, corporations, and even government agencies. In particular, cyberattacks have a serious impact on the financial sector, which is highly dependent on large amounts of stored information, data, and international transactions. Therefore, even despite the best degree of protection of large financial institutions, they are the most profitable targets for cybercriminals. At the same time, cyber threats pose the greatest danger to developing countries, while the cyber resilience of economies such as Finland, Norway, the United States, or Australia is at a high level. However, not all developing countries may be of great interest to cybercriminals. For example, Kyrgyzstan is relatively unpopular due to the low internet coverage in the country. Economic damage caused by cybercrime was estimated at USD 600 billion in 2018, USD 9.2 trillion in 2024, and is projected to reach USD 15.6 trillion by 2029.

In addition to the above, it was determined that public policy and international efforts are important for ensuring cybersecurity. Developed countries such as Finland, Norway, and Denmark demonstrate the best efforts to support cyber resilience. In particular, Finland’s updated cybersecurity strategy for 2024-2035 reflects the importance of an integrated approach to solving cyber incident response problems. Similar actions are being taken in developing countries, such as Kyrgyzstan. In 2019, a cybersecurity strategy for 2019-2023 was adopted, within the framework of which separate agencies were established and the Law on Cybersecurity was adopted. However, no subsequent national strategy has been adopted, indicating ongoing challenges in defining a medium-term vision for the development of the country’s cyber sphere. In addition, the

adoption of the UN Convention against Cybercrime in 2024 was a historic step, opening up new opportunities for coordination of actions between countries.

The limitations of the conducted research were the impossibility of obtaining information on the number of cyber incidents and convictions for them in Kyrgyzstan due to the secrecy of this data.

Future research on the topic may be based on the effectiveness of countering cyber threats within the framework of the UN Convention against Cybercrime. A comparative analysis of the level of cybercrime among the countries of the Central Asian region, or between different regions, may also be useful for the study.

Based on the conducted analysis of the main cyber threats in the context of the political and economic sphere, as well as the responses to them, a number of the following recommendations can be proposed for improving cybersecurity and reducing risks, which are suitable for implementation both at the government level and among individual business structures. The primary task should be the implementation of national cybersecurity strategies. Governments need to create long-term strategies that include comprehensive goals. Among them are the modernisation of technical infrastructure, cooperation with international partners and the private sector. The most suitable example for governments can be the Finnish model of cybersecurity support, which was adjusted in 2024 based on new threats from the Russian government. In addition, international cooperation and coordination are important aspects. Alongside efforts within the UN, it is necessary to support and be part of the activities of Interpol, Europol and other organisations engaged in the fight against cybercrime, as this threat is transnational in nature. Since cyberattacks are often aimed at disrupting the work of government agencies, governments need to invest in modernising risk management systems, training employees in methods of countering and detecting cyber threats, and implementing remote management and backup systems for critical data. What is also important is the implementation of training programmes among the population. In this context, cyber literacy courses can be introduced, which are critical for forming the concept of digital security among the public. Governments also need to address the issue of regulating the information space, but in a way that does not violate the basic democratic principles of freedom of speech. In this regard, developing countries can turn to the EU's experience in implementing laws that regulate the information space. In addition, it is necessary to establish cooperation between the public and private sectors in the field of information exchange, training, and decision-making to improve cyber protection. Also, given the rapid development of artificial intelligence, it is necessary to use this advantage to identify and prevent acts of cyberattacks, which will significantly increase the effectiveness of the fight against cybercrime.

REFERENCES

ABDYGALYM, B., SAMBETBAYEVA, M., YERIMBETOVA, A., NEKESSOVA, A., TASBOLATULY, N., SMAILOV, N., & NAZYMKHAN, A. (2025). NLP Models for Military Terminology Analysis and Detection of Information Operations on Social Media. *Computers, 14*(11), 485. https://doi.org/10.3390/computers14110485

AHMAD, W., RASOOL, A., JAVED, A.R., BAKER, T., & JALIL, Z. (2021). Cyber security in IoT-based cloud computing: A comprehensive survey. *Electronics*, *11*(1), 16. https://doi.org/10.3390/electronics11010016

AKSHATAEVA, Z., BAIZHANOVA, K., BEISEBAEVA, S., SHERIMKULOVA, G., NURAHMETOVA, G., & KHAMZINA, Z. (2016). The framework of social security system public management in Kazakhstan. *International Journal of Environmental and Science Education, 11*(18), 11645-11657. https://www.researchgate.net/publication/311603436_The_framework_of_social_security_system_public_management_in_Kazakhstan

ALIKHANOV, A.A. (2023). Economic security in the context of digitalisation as the basis for sustainable development of the regional economy. *News of Universities of Kyrgyzstan*, *1*, 122-126.

ALIKHANOV, A.A., & GYYAZOV, A.T. (2023). Theoretical foundations of ensuring economic security of the state from the point of view of sources of threats in the conditions of digitalisation. *Science, New Technologies and Innovations of Kyrgyzstan*, *4*, 171-176.

Arctic Wolf. (2025). *Top government cyberattacks*. https://arcticwolf.com/resources/blog/notable-cyber-attacks-on-government-agencies/

ASHRAF, C. (2021). Defining cyberwar: Towards a definitional framework. *Defense & Security Analysis*, *37*(3), 274-294. https://doi.org/10.1080/14751798.2021.1959141

AYUPOVA, Z. K., & SERALIYEVA, A. M. (2015). New criminal procedure code of the republic of Kazakhstan and the problems of the liberation of procedural economy, effectiveness and efficiency. *Criminology Journal of Baikal National University of Economics and Law, 9*(1), 144-153. https://doi.org/10.17150/1996-7756.2015.9(1).144-153

BAIMUHAMEDOV, M. F., ATANOV, S. K., ZHUNUSOV, K. M., ZHIKEYEV, A. A., BUGUBAEVA, A. U., & BULAEV, A. G. (2019). System of cryptographic protection of information based on deterministic chaos. *International Journal of Innovative Technology and*

Exploring Engineering, 8(12), 4495-4498. https://doi.org/10.35940/ijitee.L3527.1081219

BARLYBAYEV, A., & TURGINBAYEVA, A. (2025). Development and Implementation of an Advanced Fuzzy Expert System for the Assessment of Information Security Risks. *Journal of Computational and Cognitive Engineering, 4*(4), 570-580. https://doi.org/10.47852/bonviewJCCE52024683

BARLYBAYEV, A., SHARIPBAY, A., SHAKHMETOVA, G., & ZHUMADILLAYEVA, A. (2024). Development of a Flexible Information Security Risk Model Using Machine Learning Methods and Ontologies. *Applied Sciences (Switzerland), 14*(21), 9858. https://doi.org/10.3390/app14219858

CAVELTY, M.D., & WENGER, A. (2022). *Cyber security politics: Socio-technological transformations and political fragmentation*. London: Routledge. https://doi.org/10.4324/9781003110224

CAVELTY, M.D., ERIKSEN, C., & SCHARTE, B. (2023). Making cyber security more resilient: Adding social considerations to technological fixes. *Journal of Risk Research*, *26*(7), 801-814. https://doi.org/10.1080/13669877.2023.2208146

Centre for Strategic and International Studies (CSIS). (2024). *Significant cyber incidents*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Check Point Research (2025). *AI Security Report 2025*. https://www.checkpoint.com/resources/items/report-ai-security-report-2025

CHEN, S., HAO, M., DING, F., JIANG, D., DONG, J., ZHANG, S., GUO, Q., & GAO, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, *10*(1), 71. https://doi.org/10.1057/s41599-023-01560-x

CHIGADA, J., & MADZINGA, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1), 1-11. https://doi.org/10.4102/sajim.v23i1.1277

CHNG, S., LU, H.Y., KUMAR, A., & YAU, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

ÇIFCI, H. (2024). Analysis of Türkiye's cybersecurity strategies: Historical developments, scope, content and objectives. *Sakarya University*

Journal of Science, *28*(1), 204-219. https://doi.org/10.16984/saufenbilder.1249760

CNN. (2016). *What was in the DNC email leak?* https://edition.cnn.com/2016/07/24/politics/dnc-email-leak-wikileaks/index.html

CODREANU, C.M. (2022). Using and exporting digital authoritarianism: Challenging both cyberspace and democracies. *Europolity: Continuity and Change in European Governance*, *16*(1), 39-65.

Cybersecurity Strategy of the Kyrgyz Republic for 2019-2023. (2019). https://cbd.minjust.gov.kg/15479/edition/962966/ru

Cybersecurity Ventures (2025). *The world will store 200 Zettabytes of data by 2025*. https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/

DAHAN, E., AVIV, I., & KIPERBERG, M. (2025). Trust Domain Extensions Guest Fuzzing Framework for Security Vulnerability Detection. *Mathematics, 13*(11), 1879. https://doi.org/10.3390/math13111879

Data Breach Investigations Report. (2011). https://130e178e8f8ba617604b-8aedd782b7d22cfe0d1146da69a52436.ssl.cf1.rackcdn.com/verizon-breach-report-incidents-are-up-eresource-1-a-3559.pdf

Data Breach Investigations Report. (2015). https://doi.org/10.13140/RG.2.1.4205.5768

Data Breach Investigations Report. (2020). https://pmc.ncbi.nlm.nih.gov/articles/PMC7380945/pdf/main.pdf

DAWOOD, Y. (2021). Combatting Foreign election interference: Canada's electoral ecosystem approach to disinformation and cyber threats. *Election Law Journal: Rules, Politics, and Policy*, *20*(1), 10-31. https://doi.org/10.1089/elj.2020.0652

DEVANNY, J., MARTIN, C., & STEVENS, T. (2021). On the strategic consequences of digital espionage. *Journal of Cyber Policy*, *6*(3), 429-450. https://doi.org/10.1080/23738871.2021.2000628

Economist.kg. (2024). *Cybersecurity under threat: What crimes are most often committed in Kyrgyzstan, according to the Ministry of Internal Affairs.* https://economist.kg/novosti/2024/03/13/kibierbiezopasnost-pod-ughrozoi-kakiie-priestuplieniia-chashchie-vsiegho-soviershaiut-v-kr-rasskazali-v-mvd/

ESET Research. (2023). *A year of wiper attacks in Ukraine*. https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/

Euronews. (2023). *Russia warns of "retaliatory measures" over Finland's NATO membership*. https://www.euronews.com/2023/04/04/russia-warns-of-retaliatory-measures-over-finlands-nato-membership

Europol. (2025). EU Serious and Organized Crime Threat Assessment 2025 – AI-driven cybercrime and organized crime trends report. https://apnews.com/article/europe-crime-europol-ai-security-cyber-attack-846847536f6feb2bbb423943fd96e1f1

FALOWO, O.I., POPOOLA, S., RIEP, J., ADEWOPO, V.A., & KOCH, J. (2022). Threat actors' tenacity to disrupt: Examination of major cybersecurity incidents. *IEEE Access*, *10*, 134038-134051. https://doi.org/10.1109/ACCESS.2022.3231847

Familoni, B.T., & SHOETAN, P.O. (2024). Cybersecurity in the financial sector: A comparative analysis of the USA and Nigeria. *Computer Science & IT Research Journal*, *5*(4), 850-877. https://doi.org/10.51594/csitrj.v5i4.1046

Financial Times. (2024). *JPMorgan suffers wave of cyber attacks as fraudsters get "more devious"*. https://www.ft.com/content/cd287352-cb3b-48d8-a85b-668713b80962

Gartner. (2023). *Gartner forecasts global security and risk management spending to grow 14% in 2024*. https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024

Global Organized Crime Index. (2025). Financial and cyber-dependent crimes lead the expansion in global organized crime. *Global OC Index (GI-TOC)*. https://ocindex.net/report/2025/section2/

GULYAS, O., & KISS, G. (2023). Impact of cyber-attacks on the financial institutions. *Procedia Computer Science*, 219, 84-90. https://doi.org/10.1016/j.procs.2023.01.267

History. (2023). *Cold war history*. https://www.history.com/topics/cold-war/cold-war-history

Increase in the number of cyberattacks in 2024 and beyond. (2024). https://expert.com.ua/176744-zrostannya-kilkosti-kiberatak-u-2024-roci-i-u-podalshomu-zhytti.html

International Monetary Fund (IMF). 2024. *The last mile: Financial vulnerabilities and risks*. https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024

International Policy Digest. (2022). *How social media is fueling divisiveness.* https://intpolicydigest.org/how-social-media-is-fueling-divisiveness/

Interpol. (2025). Operation Sentinel: Interpol-led cybercrime crackdown results in 574 arrests across Africa and highlights rising cybercrime activity. https://www.tomshardware.com/tech-industry/cyber-security/interpol-led-cybercrime-crackdown-results-in-574-arrests-in-19-african-nations-decrypts-six-ransomware-variants-operation-sentinel-disrupts-rings-that-caused-usd21-million-in-losses-recovers-usd3-million

JAVAID, A. (2023). Cybersecurity: A new realm in national security of Pakistan. *Research Journal of Human and Social Aspects*, *1*(4), 52-64.

KARASHEVA, Z., ASSANOVA, S., NURAKHMETOVA, G., & NURANOVA, R. (2024). Digital (Electronic) Paid Provision of Services in the Field of Legal Activity. *Revista de Direito, Estado e Telecomunicacoes, 16*(1), 25-41. https://doi.org/10.26512/lstr.v16i1.46160

KAYODE-AJALA, O. (2023). Establishing cyber resilience in developing countries: An exploratory investigation into institutional, legal, financial, and social challenges. *International Journal of Sustainable Infrastructure for Cities and Societies*, *8*(9), 1-10.

KOVÁCS, L., & TERTÁK, E. (2024). Financial literacy is the best protection from cybercrime. *Economy and Finance*, *11*(1), 7-28. https://doi.org/10.33908/EF.2024.1.2

Law of the Kyrgyz Republic No. 121 "On Cybersecurity of the Kyrgyz Republic". (2024). https://cbd.minjust.gov.kg/4-5371/edition/13381/ru

LIU, Y. (2024). Cybersecurity risks and countermeasures in digital communication systems. *Probe-Media and Communication Studies*, *6*(2), 29-32. https://doi.org/10.59429/pmcs.v6i2.6492

MCAFEE. (2018). *Economic impact of cybercrime – No slowing down*. Washington: Centre for Strategic and International Studies (CSIS).

MCBRIDE, M. (2024). The theft of democracy in post-communist Europe: Democratic backsliding through the lens of organized crime and populist politics. *Open Journal of Political Science*, *14*(4), 653-678. https://doi.org/10.4236/ojps.2024.144036

MELAND, P.H., BERNSMED, K., WILLE, E., RØDSETH, Ø.J., & NESHEIM, D.A. (2021). A retrospective analysis of maritime cyber security incidents. *International Journal on Marine Navigation and Safety of Sea Transportation*, *15*(3), 519-530. https://doi.org/10.12716/1001.15.03.04

Microsoft. (2022). *Microsoft identified a unique destructive malware*. https://x.com/MsftSecIntel/status/1482543129454686215

MILON, M.N.U., GHOSE, P., PINKY, T.C., TABASSUM, M.N., HASAN, M.N., & KHATUN, M. (2024). An in-depth PRISMA based review of cybercrime in a developing economy: Examining sector-wide impacts,

legal frameworks, and emerging trends in the digital era. *Edelweiss Applied Science and Technology, 8*(4), 2072-2093.

Ministry for Foreign Affairs of Finland. (2023). *Cyber security and the cyber domain*. https://um.fi/cyber-security-and-the-cyber-domain

MixMode. (2024). *Global cybercrime report 2024: Which countries face the highest risk?* https://mixmode.ai/blog/global-cybercrime-report-2024-which-countries-face-the-highest-risk/

MORGAN, S. (2015). *IBM's CEO on hackers: "Cybercrime is the greatest threat to every company in the world"*. https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/

National Statistical Committee of the Kyrgyz Republic. (2024). *Criminal*. https://stat.gov.kg/en/statistics/prestupnost/

North Atlantic Treaty Organisation (NATO). (2023). *Finland joins NATO as 31st Ally*. https://www.nato.int/cps/po/natohq/news_213448.htm

OYADEYI, O.O., OYADEYI, O.A., & BELLO, R.O. (2024). Cybercrime in the Asia-Pacific region: A case study of Commonwealth APAC Countries. *Commonwealth Cyber Journal, 2*(9), 130-160.

PAANANEN, R., SOIKKELI, M., ARO, M., KUUSISTO, T., RUSILA, T., & TUULENSUU, T. (2024). *Finland's Cyber Security Strategy 2024-2035*. Helsinki: Publications of the Finnish Government.

Parliamentary Assembly of the Mediterranean. (2024). *The impact of disinformation, misinformation, fake news and foreign interference on democratic systems*. https://pam.int/wp-content/uploads/2024/10/EN-Background-paper-on-disinformation-and-fake-news-Jan-2024.pdf

PETCHENKO, I. (2024). *The number of cybercrimes in Kyrgyzstan has increased, but statistics are classified*. https://24.kg/proisshestvija/299706_chislo_kiberprestupleniy_vkyirgyizstane_uvelichilos_nostatistika_zasekrechena/

PETRAKOV, D. S., SMIRNOV, D. I., GERASIMENKO, N. N., MEDETOV, N. A., & JIKEEV, A. A. (2019). Implementation of software for data processing of X-ray optical measurements for the analysis of structural parameters. *Journal of Applied Crystallography, 52*, 186-192. https://doi.org/10.1107/S1600576718016837

Radio Free Europe (RFE). (2022). *Iranian state TV streaming site targeted with dissident message*. https://www.rferl.org/a/iran-hackers-dissident-message-tv/31683161.html

Resolution of the Kyrgyz Republic "On the Coordination Centre for Ensuring Cybersecurity of the State Committee for National Security of the

Kyrgyz Republic". (2023). https://cbd.minjust.gov.kg/159852/edition/1207958/ru

Reuters. (2016). *Behind Democrats' email leak, U.S. experts see a Russian subplot.* https://www.reuters.com/article/world/behind-democrats-email-leak-us-experts-see-a-russian-subplot-idUSKCN10609J/

REXHEPI, B. R., KUMAR, A., GOWTHAM, M. S., RAJALAKSHMI, R., PAIKARAY, M. D., & ADHIKARI, P. K. (2023). An Secured Intrusion Detection System Integrated with the Conditional Random Field For the Manet Network. *International Journal of Intelligent Systems and Applications in Engineering, 11*(3s), 14-21. https://www.ijisae.org/index.php/IJISAE/article/view/2526

RIZZONI, F., MAGALINI, S., CASAROLI, A., MARI, P., DIXON, M., & COVENTRY, L. (2022). Phishing simulation exercise in a large hospital: A case study. *Digital Health*, *8*. https://doi.org/10.1177/20552076221081716

SASI, S., & SWARNA JYOTHI, L. (2019). A novel public key crypto system based on Bernstein polynomial on Galois fields 2m to secure data on CFDP. *Smart Innovation, Systems and Technologies, 105*, 639-647. https://doi.org/10.1007/978-981-13-1927-3_67

SASI, S., SUBBU, S. B. V., MANOHARAN, P., & ABUALIGAH, L. (2023). Design and implementation of secured file delivery protocol using enhanced elliptic curve cryptography for class I and class II transactions. *Journal of Autonomous Intelligence, 6*(3). https://doi.org/10.32629/jai.v6i3.740

SHANDLER, R., & GOMEZ, M. A. (2023). The hidden threat of cyber-attacks – Undermining public confidence in government. *Journal of Information Technology & Politics*, *20*(4), 359-374. https://doi.org/10.1080/19331681.2022.2112796

SHANDLER, R., DOR, G., & CANETTI, D. (2022.) *The insidious political consequences of cyberattacks*. https://ucigcc.org/blog/the-insidious-political-consequences-of-cyberattacks/

SMAILOV, N., KADYROVA, R., ABDULINA, K., URALOVA, F., KUBANOVA, N., & SABIBOLDA, A. (2025). Application of facial recognition technologies for enhancing control in information security systems. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska, 15*(3), 55-58. https://doi.org/10.35784/iapgos.7073

State Personal Data Protection Agency under the Cabinet of Ministers of the Kyrgyz Republic. (2025). *About the agency*. https://dpa.gov.kg/ru/about

Statista. (2025). *Estimated cost of cybercrime worldwide 2018-2029*. https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

Strategy for the protection of cyberspace in Kyrgyzstan. (2024). https://digital.gov.kg/activities/strategiya-zashhity-kiberprostanstva-v-kyrgyzstane/

TASHEVA, I. (2021). Cybersecurity post-COVID-19: Lessons learned and policy recommendations. *European View*, *20*(2), 140-149. https://doi.org/10.1177/17816858211059250

Tempo. (2023). *List of developed and developing countries in the world*. https://en.tempo.co/read/1818198/list-of-developed-and-developing-countries-in-the-world

TZAVARA, V., & VASSILIADIS, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security*, *23*(3), 1695-1719. https://doi.org/10.1007/s10207-023-00811-x

United Nations (UN) *Convention against Cybercrime.* (2024). https://documents.un.org/api/symbol/access?j=N2442674&t=pdf

United Nations (UN). 2024. *Making the digital and physical world safer: Why the Convention against Cybercrime matters*. https://news.un.org/en/story/2024/12/1158526

UpGuard. (2024). *What is Ransomware as a service?* https://www.upguard.com/blog/what-is-ransomware-as-a-service

UpGuard. (2025). *The impact of cybercrime on the economy*. https://www.upguard.com/blog/the-impact-of-cybercrime-on-the-economy

WIDODO, M., ADAM, S., HSB, P.H., PRAYITNO, A.H., & BHASKORO, A. (2024). International legal dynamics in combating cybercrime: Challenges and opportunities for developing countries. *Global International Journal of Innovative Research*, *2*(1), 314-321. https://doi.org/10.59613/global.v2i1.49

World Bank Group. (2024). *Global growth is stabilizing for the first time in three years*. https://www.worldbank.org/en/news/press-release/2024/06/11/global-economic-prospects-june-2024-press-release

World Bank Group. (2025). *GDP growth (annual %)*. https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG

World Cybercrime Index. (2024). World-first cybercrime threat ranking highlights key global cybercrime hotspots. *PLOS ONE/UNSW/University of Oxford research*.

https://www.unsw.edu.au/newsroom/news/2024/04/World-first-Cybercrime-Index-ranks-countries-by-cybercrime-threat-level

World Economic Forum. (2024). *Global cybersecurity outlook 2024* (Report). Geneva: World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

ZHANZHUMENOV, R., SARGAZIN, ZH., & ESDAULETOV, N. (2022). Information policy in mass media space: case study of central Asia. *Bulletin of the Jusup Balasagyn Kyrgyz National University, 14*(3), 36-43. https://balasagynbulletin.com/en/journals/tom-14-3-2022/informatsionnaya-politika-v-prostranstvye-sryedstv-massovoy-informatsii-na-primyerye-tsyentralnoy-azii

ZHUMALIEV, A. (2022). The role of the media in updating the image of a political leader and destructive methods of its formation. *Bulletin of the Jusup Balasagyn Kyrgyz National University, 14*(1), 191-199. https://balasagynbulletin.com/en/journals/tom-14-1-2022/rol-smi-v-aktualizatsii-obraza-politicheskogo-lidera-i-destruktivnyye-priyemy-ego-formirovaniya

ZWILLING, M., KLIEN, G., LESJAK, D., WIECHETEK, Ł., CETIN, F., & BASIM, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET