Pakistan Journal of Criminology
Vol. 15, No. 04, October-December 2023 (175-192)

Criminological Aspects of the Behaviour of Victims of Cyberattacks: Case Analysis of Hacking State Organisations Ensuring National Security

Baktygul Kanybekova[1], Mamasaly Arstanbekov[2],
Bakyt Kakeshov[3], Chynybek Erdolatov[4] & Iskander Artykbaev[5]

Abstract

In an era of global use of information technology in all spheres of public life and digital delivery of all public services, the issue of protection against cyberthreats at various levels, including government organisations, is very acute. The purpose of this study was to examine aspects of victimological behaviour of victims of hacker attacks in cyberspace, represented by state organisations that ensure the national security of the country. The main methods of research were analysis and synthesis. The result of this study is an investigation of the main criminological aspects of the behaviour of victims of cybercrime and determining the role of such behaviour for committing offences in the information space, case studies of hacking of government agencies were analysed, and problematic aspects that contribute to cyberattacks were identified.

Keywords: Criminological Aspects, Cyberthreat, Cybercrime, Victim Behaviour, Information Security, Digital Space, State Bodies, National Security.

Introduction

Today, the rapid transition of all spheres of social life into the digital environment and the development of the information society is observed all over the world. Along with the technological advance, the field of crime in the information space is also evolving. Cybercrime is committed at various levels, from petty theft to hacking attacks on large businesses and government organisations. Criminologists for many decades of research into the mechanism of committing classic crimes have already fully studied the personality of the victim and the perpetrator, the causal links between the characteristics of the victim and the commission of a particular crime. However, dynamic scientific and technological

[1] Department of Theory and History of State and Law, Kyrgyz National University named after Jusup Balasagyn, Bishkek, Kyrgyz Republic.
[2] Department of Criminal Law and Process, Osh State University, Osh, Kyrgyz Republic.
[3] Department of Criminal Law and Criminology, Kyrgyz National University named after Jusup Balasagyn, Bishkek, Kyrgyz Republic. bakytkakeshovv67@gmail.com
[4] Department of Criminal Law and Process, Osh State University, Osh, Kyrgyz Republic.
[5] Department of Criminal Law and Criminology, Kyrgyz National University named after Jusup Balasagyn, Bishkek, Kyrgyz Republic.

advance is presenting criminologists with new challenges. Because, due to the specific use of cyberspace and the very rapid pace of its development, the identity of the victim of cybercrime is still very understudied. Internet crime is currently remarkably diverse, and therefore cyberdefence and countering crime in the information space is one of the priority areas of state security in general (Serikova et al., 2022). Government agencies play a key role in implementing protection measures in the virtual environment, as due to widespread digitalisation, it is government organisations that hold most citizens' personal data that can be exposed to cyberthreats (Jatkiewicz, 2013; 2023). That is why the analysis of criminological aspects of the behaviour of victims of cyberattacks, specifically of state bodies, which are constantly exposed to danger from cybercriminals, is truly relevant and necessary for the creation of a unified strategy of information security of the state. It is the detailed study of the information and cyberpolicy behaviour of civil servants and public bodies in general that will help to identify some of the weaknesses in the public sector. The study of the criminological characteristics of the victim will help to pinpoint an effective strategy to prevent cybercrime, which is increasing day by day and already constitutes a major threat to national and state security.

The problematic of the study is that with the emergence of new legal relations it is necessary to properly regulate them. As criminal acts are taking on new forms and methods against the backdrop of the rapid growth of information services, one of the fundamental issues is the study of the behaviour of participants in cybercrime, namely, the analysis of the victimological behaviour of victims of such offences (Kerimkhulle et al., 2023). While the victimisation behaviour of ordinary citizens in cybercrime is obvious, the behaviour of government agencies that are responsible for ensuring cybersecurity needs to be analysed and studied in detail. As specialised skills are required to carry out a crime of this level, specific knowledge is also required to implement security measures that will help build a holistic cybersecurity system. Some Kyrgyz scholars have investigated this subject. A.M. Tashbaev et al. (2022) studied the problem of developing the digital skills of the population in the context of the need to apply measures to develop the economic potential of the country and preventive measures against cybercrime.

Kyrgyz scientist D.G. Tugolbaev (2018) in a scientific paper considered some problematic aspects of information security in the Kyrgyz Republic. The author analyses the state of the information system, weaknesses of its protection and identifies certain areas for the development of the information environment security sphere. The author examines in detail the legislative acts regulating the issues of information security in Kyrgyzstan, analyses the term "information security" and compares it with other definitions in this sphere. The approval in June 2012 by the Decree of the President of the Kyrgyz Republic of the new edition of the Concept of National Security of the Kyrgyz Republic was a major step towards the development of an adjusted state strategy in the field of national security. As noted by the U.S. Zhumabaev (2015), ensuring national security is understood as the activities of state and public institutions, as well as citizens to identify, prevent, and counter threats to security. The author emphasises that in the legislation of the Kyrgyz Republic there is no clear definition of the concept of ensuring national security, which complicates the activities of government agencies in this area. In this regard, the researcher proposes to supplement the law with a concrete definition of this concept.

Kyrgyz scientists R.M. Toksonalieva and G.S. Musurmanova (2018) also investigated the impact of modern information and communication technologies on the development of information society in Kyrgyzstan. In their opinion, ICTs have a considerable impact on the social structure of society, the economy, and political institutions. The authors note that in Kyrgyzstan there is an active penetration of digital technologies in all spheres of life, including public administration and business. However, a full-fledged transition to the information society is still difficult due to the uneven access of the population to ICTs. R.M. Toksonalieva (2015) considers the problems of ensuring information and psychological security of Kyrgyzstan. In the author’s opinion, the state policy in this sphere is not systematic enough. The researcher notes the vulnerability of society to external information-psychological influence and the need to develop a comprehensive state programme to counter such threats. Special attention is paid to training in strategic analysis and information-psychological defence (Zhakupov et al., 2023). Thus, the author emphasises the importance of information and psychological security for the national interests of Kyrgyzstan.

A.O. Bukueva (2020) reviewed the current state of cybersecurity in Kyrgyzstan, and the author identified the main risks that may be relevant in the near future for the information security of the entire country and identified the main areas of state policy in the field of ensuring cybersecurity. Kyrgyz researcher A.M. Ismailakhunova (2023) investigated the specific features of digital development of the Kyrgyz economy. This paper reviewed the main documents regulating technological development in the country and analysed the advantages and disadvantages of digitalisation in the Kyrgyz Republic. The scientist emphasised that the digitalisation of social processes is inevitable, and therefore the reform of the national economy should be approached in an integrated manner. N.Zh. Zhusuyeva and Zh.S. Samatova (2020) studied the specific features of information security in the banking sector. The paper examined the diverse types and kinds of cyberthreats in the banking industry and analysed their impact on bank operations using particular examples. Z.R. Kazanbaeva (2019) considered some problematic aspects of cybersecurity in the Kyrgyz Republic. The paper identified the main trends in the development of cyberthreats in the modern information space and outlined the necessary measures to curb such threats. Having studied the works of Kyrgyz scholars, it should be noted that cybersecurity research is either very narrow, dealing only with specific sectors, or, conversely, extremely broad, outlining general aspects of cybersecurity. Among the studies, there are no scientific studies that provide a detailed criminological characterisation of cybercrime and the persons who are its subjects.

The purpose of this study was to conduct an analysis of the criminological characteristics of the behaviour of victims of cyberattacks, namely state authorities that provide security at the national level, in the context of the impact of such behaviour on the causes and consequences of the commission of a crime in the digital space. The tasks of this study were to identify the main characteristic features of victims' behaviour, to analyse specific cases of cyberattacks on state bodies, to carry out a comparative analysis of the conditions of committing crimes in cyberspace with another country, namely Ukraine, to identify weaknesses in the behaviour of the apparatus of state bodies in the field of information security.

Materials and Methods

Using the formal-logical method, the current state of information security in the country was studied, and the problems and challenges that have appeared before society as a result of technological advance were consistently investigated. The analysis method was used to identify the main criminological features of the behaviour of victims of cyberattacks, to examine some cases of hacking and establish a causal relationship between the behaviour of victims and the number of cybercrimes committed, and to formulate practical recommendations for the prevention of cyberattacks and their consequences for affected individuals. Using the synthesis method, various aspects of the victim's personality were studied and combined into a single criminological characteristic, and practical steps for improving the behaviour of individuals at cyberthreats were identified using synthesis. Using the method of induction, by examining case studies of cybercrime, a conclusion was reached on the main problems and challenges faced by public authorities in implementing cybersecurity measures.

Based on the method of deduction, using the general knowledge of criminological features of crime victims, the specific features of the behaviour of crime victims in cyberspace were identified, and the criminological features of the behaviour of exactly the state bodies in the field of security were determined. The historical method made it possible to investigate some cases of large-scale cyberattacks that targeted security agencies and government bodies in the recent past to illustrate the mechanism of cybercrime at the state level. Using the method of concretisation, certain types of cybercrime with a specific victim-side actor were studied, and concrete cases of cyberattacks on state bodies ensuring national security were examined as examples. Using analogy, the same characteristics of cybercrime victim behaviour in different states were investigated. Using the method of comparison, the criminological features of the behaviour of victims of cyberattacks in Ukraine were studied, and the state of the information security system in Kyrgyz Republic and Ukraine was compared. The generalisation method was used to identify common problematic behaviours that are common to victims of cybercrime in all countries and to identify common rules of conduct for actors to prevent cyberattacks.

Results

Criminological features of the behaviour of victims of cyberattacks in the Kygyz Republic

Today, all the processes of citizens' life activities are moving to the information plane, starting from financial transactions and ending with small civil law transactions. Public services and the activities of public authorities are no exception, which are also digital in nature. Along with the positive aspects of information technology advances, there has also been an increase in the use of IT for the purpose of committing criminal offences (Spagnolli et al., 2022). As the digitalisation of society is gaining very rapid momentum, cybercrime can occur at distinct levels and on different scales. Recently, the number of targeted cyberattacks has increased worldwide. And it is worth noting that 86% of all targeted attacks were completely against different organisations. Specifically, government agencies were the most frequently attacked (16% of all cyberattacks) (Bout et al., 2021). The rapid development of the digital environment facilitates the emergence of the latest schemes and methods of cybercrime, and therefore, effective counteraction requires a clear understanding of the mechanism of committing crimes in the electronic environment and the characteristic behaviour of both the offender and the victim of this offence (Holt, 2019).

As early as 2020, Kyrgyzstan's policy was aimed at full digitalisation of state and municipal services (State Portal of Digital Services of the Kyrgyz Republic). Much attention has been paid to those bodies that ensure state security. Despite quite positive results in the transition of all spheres of life of citizens to digitalisation, the problem of cybersecurity is still truly relevant for Kyrgyzstan, especially in the sphere of activities of state bodies. Hacker attacks on official websites of government agencies and the country's top officials are becoming more frequent, which is a threat to the protection of personal data of millions of citizens. To achieve their goal, cybercriminals use various innovative technical means as well as manipulative techniques that psychologically influence the potential victim (Ainutdinova & Ainutdinova, 2022). At first glance, it may appear that the victim of any cyberattack could be an incompetent individual who has little familiarity with innovative technology. However, based on the fact that the victims of cybercrime are also qualified employees of different services and agencies, as well as professionals who are directly involved in information security, it can be argued that the identity of the victim of attacks in cyberspace cannot be characterised by specific attributes such as gender, age, occupation (Cazares et al., 2023). Any person can be a victim of such offences, regardless of their professional qualities. Due to the large amount of information that is available on the Internet, it is often possible for attackers to learn a lot of valuable information about a victim, using it to launch a cyberattack. A feature of cybercrime is that victimisation of the victim occurs very spontaneously and, in most cases, with voluntary consent. Individuals who are subjected to cyberattacks may not realise the nature of the particular situation at hand (Dralova, 2021).

The main problem with cyberattack victim behaviour at any level is digital illiteracy. Unfortunately, this characteristic is also inherent in the personnel of public bodies. To date, steps are being taken to achieve global standards in the field of information security at the state level, but so far the level of protection is only countering standard threats (Dumchykov et al., 2022). Since cybersecurity and information security are among the key tasks of the state to ensure national security in the current realities, several reasons for the victimisation behaviour of cybercrime victims represented by state agencies should be highlighted. Firstly, digital illiteracy of civil servants does not imply poor technical training. What this definition means is that at the state level, a unified notion of information and cybersecurity does not always persist among government officials. Often, even leading IT professionals reduce information security measures solely to the application of technical means, such as antivirus or protecting the computer from malware (Makhazhanova et al., 2022; Breus and Khaustova, 2016). This approach is outdated as the development of information technology has brought new risks and challenges. Therefore, cybersecurity, IT security, and information security should be separated. Information security is the protection of any data, including conventional paper-based data. Cybersecurity encompasses the protection of digital data in the digital space. IT security includes activities of a technical nature, which are aimed at ensuring the protection of the computer from external intrusions (Ismailova, 2017).

When investigating the criminological features of cyberattacks on government agencies, these crimes are not simply aimed at causing harm to specific individuals or organisations. Such cyberattacks are damaging to the entire nation and the consequences can be unforeseeable. Therefore, when analysing the behaviour of cybercrime victims represented by governmental organisations, different influences on them should be considered (Bossler, 2021). For a considerable period, Kyrgyz Republic was among the top three countries that are subject to cyberattacks. The aim of the attackers is to gain access to documents held by a particular government organisation. Of particular interest for hacker targeted attacks are bodies that ensure national security in the Kyrgyz Republic, such as the Ministry of Internal Affairs, the Ministry of Defence, the State Committee for National Security, the Ministry of Digital Development, the State Border Guard Service, and others. For example, in 2013, the websites of all law enforcement agencies in Kyrgyzstan were subjected to a serious cyberattack, after which internet resources were inoperable for a long time (Hackers attacked websites of security forces of Kyrgyzstan, 2023). Government authorities in all Central Asian countries, including the Kyrgyz Republic, were subjected to a massive cyberattack in 2016. The hacker criminal group Danti was involved in this attack. The criminals used a vulnerability in a Microsoft Office application to hack into websites and cyber-espionage. The attackers used a piece of software or programme code that they spread via phishing emails asking people to open a message (Leonow et al., 2019). To convince the recipient to open the email, the attackers use the names of high-ranking officials as senders. As soon as the software is run on the victim’s device, then a program is triggered on the system giving full access to sensitive data of a government organisation. Furthermore, it is exceedingly difficult to detect an attack because the programming code used by attackers is very complex and can disguise itself from standard Windows defences. In addition, a major hacker attack in 2017 that affected most of the official websites of government agencies became known (Kobets, 2022).

As early as 2023, Kyrgyzstan experienced a wave of imaginary mines at educational institutions. The police started to receive reports of mined higher and secondary educational institutions. According to the results, these were purely psychological attacks aimed at spreading panic and fear among the population. These cyberattacks were quite massive and prolonged, as several sites were reported to be mined at the same time. In Bishkek alone, there were three such attacks in April 2023, and according to statistics from the country’s Interior Ministry, as of 1 October 2023, the police had already received 181 calls about false cases of mines.

Psychological attacks of this kind have profoundly serious consequences, as they target the most vulnerable segments of the population – children and their parents. Stopping the educational process, forced evacuation measures have an adverse impact on the moral and psychological state of children. Such false alarms reduce trust in law enforcement and increase the risk of not taking the real terrorist threat seriously. Since teachers and school administrators are responsible for the safety of pupils, they are obliged to take all appropriate measures to ensure that children are in a safe place. Although, due to such massive cyberattacks, everyone realises that the bombing is actually a false alarm, teachers take evacuation measures and children leave the school premises every time. The same approach applies to the activities of law enforcement agencies. Police officers are obliged to verify the information that has been received from the perpetrators and to make sure that there is no real threat to the public, even if the falsity of such reports is clear. According to media reports, law enforcement agencies have so far been unable to identify the organisers of cyberattacks on educational institutions because the perpetrators use disposable emails registered in other countries, indicating that the mechanism for countering cyberterrorism that currently exists in Kyrgyzstan is imperfect (Psychoterrorism in Bishkek: Who is trying to intimidate Kyrgyzstanis and why, 2023).

By analysing some cases of hacking of government websites, it is possible to identify several factors that influence the target’s victimhood in this case. All factors can be roughly divided into technical and human factors. Technical factors should include the availability of proper software that can respond to cyberattacks, the technical capability to investigate cybercrimes, and the existence of a unified strategy to combat and prevent cyberterrorism in the state (Gupta, 2023). In addition, the human factor cannot be underestimated when committing offences in cyberspace over state structures. Often the cause of successful cyberattacks is digital illiteracy of employees and the lack of a systematic approach to regulating cybersecurity in government agencies. In most cases, attackers take advantage of the trust of a government employee who opens emails from unverified sources without proper attention and provides a full opportunity to steal sensitive data (Babak et al., 2021).

Due to the large-scale digitalisation of public administration and the growth of cyberthreats to all users, it is necessary to implement preventive measures based on global experience. First and foremost, preventing cyberattacks and the aftermath is closely linked to improving the digital literacy of citizens. Furthermore, effectively countering cybercrime requires a government strategy, which may include a technical and organisational component. The combination of modern technical support and conscious use of information resources will allow the Kyrgyz Republic to achieve prominent results in cybersecurity.

Criminological features of the behaviour of victims of cyberattacks in Ukraine

With the emergence of new scientific and technological solutions, there are also new risks and threats to data security at various levels. However, under martial law, which has been in effect in Ukraine since February 2022, the level of such threats increases tenfold. Despite this, the public administration system is functioning and almost all public services are provided to citizens in digital format. For this reason, Ukraine's experience in countering and preventing cybercrime is very illustrative. In the context of hybrid warfare, with a strong focus on military action and in the information space, government agencies, and especially those that provide national security, are a prime target for cyberterrorism. Threats can be both inside and outside the organisation and can have very devastating consequences that substantially reduce the level of defence capability of a country. Therefore, as of today, society and government agencies are forced to change their behavioural pattern to find innovative solutions to ensure that they can counter multiple cyberattacks (Akhmetzhanova et al., 2023).

For many years, Ukraine has lacked a system of proper legal regulation of information security, specifically cybersecurity. The weak legal regime has created a favourable environment with a low legal and information culture and many manifestations of irresponsibility. Ukrainian society, as well as citizens of other countries, is characterised by low digital literacy, excessive trustworthiness, irresponsible attitude towards the protection of their personal data (Mykhaylenko, 2020). Considering the human factor in the context of the work of employees in public bodies, one can also identify some features of victim behaviour, namely: low level of professional knowledge, due to insufficient funding, very often public servants reveal a desire to reduce time and resources in the performance of their obligations, which can lead to criminal negligence and provide additional opportunities for attackers to carry out a cyberattack (Yedharov, 2021). In addition, due to low financial incentives for civil servants, internal cyber-espionage, where a cyberthreat is manifested from within an organisation, has become quite common. Under such circumstances, cyberthreats are even more dangerous and can cause dozens of times more harm (Maltseva et al., 2022).

Considering the behaviour of state bodies as representations of state power in a broader sense, it is worth noting that the lack of technical support and organisational basis for preventive measures in cybersecurity further reinforce the victimisation component of cybercrime in which state bodies become victims. But as active military operations began in 2022 and cyberattacks became massive, Ukrainian civil society began to realise the importance of cybersecurity and its place in the integrity and security of the country. Since modern warfare has acquired a hybrid nature, many special operations occur precisely in the information space.

These cyberattacks are not aimed at ordinary citizens and their personal data. Hacker breaches have occurred and continue to occur on critical infrastructure and jeopardise the functioning of an entire nation. After February 2022, the Ukrainian government had to take urgent action to keep critical state facilities under control, as well as adopt an overall follow-up strategy to minimise the impact from future cyberattacks. A vital role in the preventive mechanism of countering cybercrime was played by a broad information campaign, which made it possible to prepare the population for information attacks from the aggressor.

Notably, government agencies providing national security are faced with a global and complex offence as cyberterrorism. While hacking is technically correctable, cyberterrorism aims to spread panic among the population, leading to unforeseeable losses, both informationally and materially (Babak et al., 2020). When conducting a criminological characterisation of the victims of such crimes, it is worth noting that, compared to Kyrgyzstan, there has been some progress in Ukraine in terms of behaviour in the face of the cyberthreat. As in other countries, victimisation behaviour in Ukraine is also influenced by various kinds of factors: human and technical. Some changes should be attributed to the specific features of subjective behaviour of employees of state bodies, such as manifestations of greater attention to extraneous addressees and unverified information messages, more responsible attitude towards professional duties in the field of security. On the technical side, government agencies have also started to look for alternative solutions to minimise the risks of cyberattacks. One such solution is the use of Security Information and Event Management (SIEM). These systems collect incident information from various standard defence systems and allow the identification of suspicious and potentially dangerous situations. Furthermore, the use of such systems can substantially reduce the time to identify security risks and reduce security costs. This system can be placed either on the user’s network or remotely. The value of such systems is that it collects information from all devices and produces data available for analysis. The use of ultramodern defence systems and early detection of cyberthreats considerably contribute to cybersecurity.

In the context of warfare and constant cyberattacks on government agencies, the demand for remote activity tools, including e-services, has increased significantly. The solution that has solved this problem is the use of cloud storage. It is with the help of cloud solutions that public authorities can carry out an uninterrupted process of public administration, avoid purchasing their own servers and substantially reduce costs from the state budget. Cloud infrastructure is a priority in the development of information infrastructure in the future as it provides security and agility in the delivery of digital public services (Shevchenko, 2023). Having analysed the specifics of victim behaviour in cyberattacks, it can be argued that in most cases the victim behaviour of targets of such attacks is expressed in the same way. Even when cybercrime is committed by specialised bodies that have a duty to ensure information security, the human factor plays a crucial role. The security of the public institution and the state as a whole depends on how responsibly and professionally an employee approaches their duties (Meurs et al, 2022).

Considering all the problematic aspects related to the victimisation behaviour of individuals who are exposed to cyberthreats, several universal areas for the development of information culture and cybersecurity can be identified. Information education can be identified as one of the priority areas, as special knowledge will help to recognise the cyberthreat at an early stage and help to avoid devastating consequences (Karabayev et al., 2023). Furthermore, the availability of digital literacy will contribute to the formation of a legal culture in the information space. It is also crucial to have a relevant and functional legal framework that can ensure the existence of a unified mechanism for the prevention of cybercrime, as well as ensure the establishment of liability for offences in the information space. For an effective cybersecurity system to exist, there must be one strategy with the same approaches to address different challenges in an era of rapidly evolving cyberspace, and concepts related to cybersecurity must be fixed and delineated at the state level. And the key role in ensuring information security is played by the technical component, which provides the technical ability to counter cyberattacks of various kinds. Only the combination of all factors will help to build a reliable international level cyberdefence system.

Discussion

For a complete and comprehensive investigation of the subject, scientific articles by Kyrgyz and international authors who carried out their scientific activities in the field of cybercrime were used. Thus, a group of American scientists T.E. Dearden et al. (2023) investigated the criminological characteristics of businesses that suffered from cyberattacks, the work compares crimes that were committed by internal or external persons, analyses diverse types of cybercrime. The authors investigated the factors of mitigating the risks of insider attacks in enterprises, studied the statistics of such attacks between different entities and the consequences of them. This study has helped to identify the main criminological features and logic of the behaviour of the victim of crime in cyberspace, when the victim is not just an ordinary user, but an entire enterprise or organisation. At the same time, the study focuses all its attention on private enterprise without considering the specific features that characterise public institutions.

A. Hutchings et al. (2019), in their book, which focused on the human factor in cybercrime, investigated in detail the latest techniques and methods by which attackers deceive the most robust defences. The authors point out that standard defence mechanisms against various cyberthreats are no longer a panacea. The authors reveal in detail the criminological characteristics of cybercrime and study the personality of the perpetrator, define the main definitions and differentiate cybercrime. Using this book, the role and importance of the human factor in the mechanism of cybercrime has been defined and the main ways in which criminals deceive defence systems have been explored. American researchers T.E. Dearden and P. Gottschalk (2023) analysed cybercrime on the Internet in their study, putting forward the theory of convenience of cybercrime. In this way, the authors explain how modern technologies have created the opportunity and motive to commit new types of crime. The paper points out that modern technologies have created a favourable environment for committing financial crimes in the cyber-environment. The authors argue that cryptocurrency offences are accompanied by opportunity, intent, and motive. These components were tested on a sample of United States adults and all three were found to be characteristic of financial cybercrime (Kerimkhulle et al., 2022).

A. Morgan and I. Voce (2022) investigated cybercrime victimisation, using survey data to analyse the prevalence of data breaches among Australian users and their relationship to different criminological factors in cybercrime. The paper found that nearly one in ten respondents said their data had been disclosed. A third of this number of interviewees were victims of other cybercrime involving personal data. The authors investigated the relationship between the victimisation behaviour of such individuals and the perpetration of fraud against them in a virtual environment. As a result of the study, the researchers concluded that measures to protect individuals whose information has been disclosed are crucial and are prioritised in case of a data breach.

British researchers S. Kemp et al. (2023) investigated the influencing factors on cybercrime reporting, specifically those factors that affect victims’ reporting of a cybercrime incident. The paper analyses research into UK cybersecurity breaches to examine the factors behind the rise in cybercrime by private enterprises. The reasons for reporting or not reporting an information security offence against private businesses are also determined. And according to the results of the study, it was found that the actions of businesses depend on the type of cybercrime and the negative consequences to which such an offence has led. The authors paid considerable attention to the criminological factors of cyberthreat behaviour of businesses, and the paper also discussed the role of the private cyberdefence sector in the overall security domain.

When studying the criminological features of cybercrime, most authors conclude that the principal factor of cybercrime is digital illiteracy and information irresponsibility (Babenko et al., 2023). Researchers say that due to very rapid technological advance, most countries have not yet developed a culture of behaviour in virtual space. Along with the low digital literacy of society in general, there is also low qualification of employees of state organisations and law enforcement agencies. In most cases, scientists consider in their scientific studies the criminological aspects of the behaviour of victims as ordinary citizens, analysing cybercrimes such as cyberfraud. There are very few studies that analyse the victimisation behaviour of government agencies as victims of cyberterrorism. All studies concerning the criminological characterisation of this type of crime are aimed at identifying recommendations for concrete actions to improve the level of information security.

The limitations of this paper are that the criminological analysis of victim behaviour has only been conducted in relation to state organisations that provide national security. Only some of the most notorious cases of hacking of security agencies were considered, as there have been so many such cyberattacks. To compare and identify both positive and negative aspects, the specific behaviour of victims of cyberattacks of the two countries was examined and no attention was paid to the study and analysis of international cybersecurity standards.

Conclusions

According to the findings of this study, due to the global digitalisation of all social processes, cybersecurity has become one of the key components of the national security of the state. As government agencies are key to information security and hold sensitive information, cyberdefence of organisations performing government functions must be at the highest level. Many circumstances influence the mechanism by which a crime is committed in cyberspace, including the target's victimisation behaviour, which makes it easier for perpetrators and exacerbates the consequences. The behaviour of public authorities and their employees in the criminological aspect also depends on a range of factors, such as technical capabilities, the existence of a legislative and organisational framework, and the human factor, which includes digital literacy and professionalism. Today, in most countries, specifically in Kyrgyzstan and Ukraine, the main problem of behaviour in cyberspace is the lack of a culture of behaviour on the Internet, the lack of special knowledge and training to respond quickly to cyberthreats, and the excessive gullibility and irresponsibility of public servants. Very often, targets of cybercrime underestimate the capabilities of cybercriminals and rely only on standard defence systems, resulting in massive losses.

A promising area for further research is to investigate in greater detail the types of cybercrime and their criminological characteristics, including victim and perpetrator behaviour. It is also important to identify concrete practical recommendations for improving government policy in the area of cybersecurity. Furthermore, it is still promising to study the practical experience of countering cyberthreats of those countries that have achieved considerable success in cybersecurity according to global standards. As a result of the study, the objectives were achieved. Namely, the behavioural characteristics of state organisations as victims of cyberattacks were analysed. Particular cases of hacking of government websites were analysed and the main factors on the part of the victim that influence the possibility of committing cybercrime were identified.

References

Ainutdinova, K.A. & Ainutdinova, I.N. (2022). Victimological features of cybercrime in the context of digital transformation of society. In: Mat*erials of the All-Russian Scientific and Technical Conference* (pp. 34-39). Kazan: University of Management “TISBI”.

Akhmetzhanova, A.Kh., Mukhanova, G.Kh., Nazikova, Z.A., Malaeva, R.A. & Beisekova, Z.I. (2023). Economy and Management of an Innovative Enterprise. *International Journal of Interdisciplinary Organizational Studies,* 18(1), 119-131.

Babak, V.P., Babak, S.V., Eremenko, V.S., Kuts, Y.V., Myslovych M.V., Scherbak, L.M. & Zaporozhets, A.O. (2021). Models of Measuring Signals and Fields. *Studies in Systems, Decision and Control*, 360, 33-59.

Babak, V.P., Babak, S.V., Myslovych, M.V., Zaporozhets, A.O. & Zvaritch, V.M. (2020). Methods and models for information data analysis. *Studies in Systems, Decision and Control*, 281, 23-70.

Babenko, V., Chukurna, O.U., Niekrasova, L., Stanislavyk, O., Tyukhtenko, N., Lytvynenko, O. & Davydko, S. (2023). Methodology for Assessing the Risk of Implementing the Strategy of Diversification of Enterprises in the Aspects of Information Technology Management. *Journal of Information Technology Management*, 15(1), 192-207.

Bossler, A.M. (2021). Neutralizing cyber-attacks: Techniques of neutralization and willingness to commit cyber-attacks. *American Journal of Criminal Justice*, 46, 911-934.

Bout, E., Loscri, V. & Gallais, A. (2021). How machine learning changes the nature of cyberattacks on IoT networks: A survey. *IEEE Communications Surveys & Tutorials*, 24(1), 248-279.

Breus, S.V. & Khaustova, Y.B. (2016). Balanced scorecard system application in the activities of higher education institutions. *Actual Problems of Economics*, 183(9), 109-116.

Bukueva, A.O. (2020). Kyrgyzstan's cybersecurity. *Bulletin of the Academy of Public Administration under the President of the Kyrgyz Republic*, 27, 294-298.

Cazares, M., Fuertes, W., Andrade, R., Ortiz-Garcés, I. & Rubio, M.S. (2023). Protective factors for developing cognitive skills against cyberattacks. *Electronics*, 12(19), 4007.

Dearden, T.E. & Gottschalk, P. (2023). Convenience theory and cybercrime opportunity: An analysis of online cyber offending. *Deviant Behavior*. https://doi.org/10.1080/01639625.2023.2246626

Dearden, T.E., Parti, K., Hawdon, J., Gainey, R., Vandecar-Burdin, T. & Albanese, J. (2023). Differentiating insider and outsider cyberattacks on businesses. *American Journal of Criminal Justice,* 48(4), 871-886.

Dralova, O.M. (2021). Victimological characteristics of cybercrimes. In: *Collection of materials of the International Scientific and Practical Conference "Crime in the CIS: Problems of Prevention and Discovery of Crime"* (pp. 245-246). Voronezh: Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation.

Dumchykov, M., Utkina, M. & Bondarenko, O. (2022). Cybercrime as a threat to the national security of the Baltic States and Ukraine: The comparative analysis. *International Journal of Safety and Security Engineering*, 12(4), 481-490.

Gupta, T. (2023). Emerging trends of cybercrime in India: A contemporary review. *Journal of Law and Policy Transformation*, 8(1), 57-65.

Hackers attacked websites of security forces of Kyrgyzstan. (2023). Retrieved from https://rus.ozodi.org/a/24908150.html

Holt, T.J. (2019). *The human factor of cybercrime*. London: Routledge.

Hutchings, A., Pastrana, S. & Clayton, R. (2019). Displacing big data: How criminals cheat the system. In: *The Human Factor of Cybercrime* (pp. 408-424). London: Routledge.

Ismailakhunova, A.M. (2023). Features of digital development of the economy of Kyrgyzstan. *Greater Eurasia: Development, Security, Cooperation*, 2-3, 120-123.

Ismailova, R. (2017). Web site accessibility, usability, and security: a survey of government web sites in Kyrgyz Republic. *Universal Access in the Information Society*, 16, 257-264.

Jatkiewicz, P. (2013). Identifying factors of an information security management system of local self-government bodies. *Lecture Notes in Business Information Processing*, 161, 50-65.

Jatkiewicz, P. (2023). An Attempt to Define the Concept of Entertainment 4.0 by Analogy to other Concepts, e.g., Industry 4.0, Education 4.0, etc. *Economic Affairs (New Delhi)*, 68, 773-779.

Karabayev, S., Nurgaliyeva, K., Kredina, A., Bekturganova, M. & Aimagambetov, Y. (2023). Relationship between determinants of higher education and economic development: The case of kazakhstan. *Problems and Perspectives in Management*, 21(1), 336-351.

Kazanbaeva, Z.R. (2019). Some cybersecurity issues in the Kyrgyz Republic. *Matters of Russian and International Law*, 9(10), 493-500.

Kemp, S., Buil-Gil, D., Miró-Llinares, F. & Lord, N. (2023). When do businesses report cybercrime? Findings from a UK study. *Criminology & Criminal Justice*, 23(3), 468-489.

Kerimkhulle, S., Baizakov, N., Slanbekova, A., Alimova, Z., Azieva, G. & Koishybayeva, M. (2022). The Kazakhstan Republic Economy Three Sectoral Model Inter-sectoral Linkages Resource Assessment. *Lecture Notes in Networks and Systems*, 502 LNNS, 542-550.

Kerimkhulle, S., Saliyeva, A., Makhazhanova, U., Kerimkulov, Z., Adalbek, A. & Taberkhan, R. (2023). The estimate of innovative development of construction industry in the Kazakhstan. *E3S Web of Conferences*, 389, 06004.

Kobets, P.N. (2022). Characteristics of modern features of illegal activities committed in cyberspace. *Modern Science*, 3, 18-21.

Leonow, A.I., Koniagina, M.N., Petrova, S.V., Grunt, E.V., Kerimkhulle, S.Y. & Shubaeva, V.G. (2019). Application of information technologies in marketing: Experience of developing countries. *Espacios*, 40(38).

Makhazhanova, U., Kerimkhulle, S., Mukhanova, A., Bayegizova, A., Aitkozha, Z., Mukhiyadin, A., Tassuov, B., Saliyeva, A., Taberkhan, R., Azieva, G. (2022). The Evaluation of Creditworthiness of Trade and Enterprises of Service Using the Method Based on Fuzzy Logic. *Applied Sciences (Switzerland)*, 12(22), 11515.

Maltseva, I.R., Chernish, Y.O. & Shtonda, R.M. (2022). Analysis of some cyber threats in war. *Cybersecurity: Education, Science, Technique*, 4(16), 37-44.

Meurs, T., Junger, M., Tews, E. & Abhishta, A. (2022). Ransomware: How attacker's effort, victim characteristics and context influence ransom requested, payment and financial loss. In: *2022 APWG Symposium on*

Electronic Crime Research (eCrime). https://doi.org/10.1109/eCrime57793.2022.10142138

Morgan, A. & Voce, I. (2022). *Data breaches and cybercrime victimisation.* Canberra: Australian Institute of Criminology.

Mykhaylenko, V.V. (2020). Separate issues of victimological prevention of cybercrimes. In: *Materials of the 20th All-Ukrainian Scientific Conference on Criminology for Students, Postgraduates and Young Scientists "Criminals and Victims of Crimes"* (pp. 441-444). Kharkiv: Yaroslav the Wise National Law University.

Psychoterrorism in Bishkek: Who is trying to intimidate Kyrgyzstanis and why? 2023. Retrieved from https://stanradar.com/news/full/52264-psihoterror-v-bishkeke-kto-i-zachem-pytaetsja-kyrgyzstantsev-zapugat.html

Serikova, M., Sembiyeva, L., Orozonova, A., Tazhikenova, S., Kuchukova, N. & Mikhailova, G. (2022). The Impact of Performance Improvement of the Tax System on the Economic Growth of Developing Countries Based on the Experience of the European Union. *Montenegrin Journal of Economics*, 18(4), 203-214.

Shevchenko, V.M. (2023). The use of cloud technologies as a factor in the smooth implementation of service activities by state administration bodies. In: *Materials of the 4th International Scientific and Practical Internet Conference "Pathways to the Development of Science in the Conditions of the Modern Crisis"* (pp. 450-451). Dnipro: WayScience.

Spagnolli, A., Masotina, M., Scarcia, A., Zuffi, B. & Gamberini, L. (2022). How to get away with cyberattacks: An argumentative approach to cyberattacks' legitimization by common users. In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems.* https://doi.org/10.1145/3491102.3517444

Tashbaev, A.M., Osmonalieva, D.A. & Zhakshylyk kyzy, G. (2022). Development of digital skills in the context of implementation of digital projects in the Kyrgyz Republic. *Journal of Economy and Business*, 1-2(83), 74-80.

Toksonalieva, R.M. & Musurmanova, G.S. (2018). The influence of modern information and communication technologies on the development of the information society of Kyrgyzstan. *Theory Science*, 5, 133-140.

Toksonalieva, R.M. (2015). Public policy of Kyrgyz Republic in sphere informational-psychological of security. *Bulletin of the Kyrgyz-Russian Slavic University*, 15(5), 35-38.

Tugolbaev, D.G. (2018). Several aspects and problems of ensuring information security of the Kyrgyz Republic. *Bulletin of the Academy of Public Administration under the President of the Kyrgyz Republic*, 24, 265-274.

Yedharov, A.R. (2021). Some criminological aspects of cybercrime prevention. *Irpin Legal Journal*, 1(5), 184-191.

Zhakupov, Y.K., Berzhanova, A.M., Mukhanova, G.K., Baimbetova, A.B. & Mamutova, K.K. (2023). The impact of entrepreneurship on the socio-economic development of regions. *Business Strategy and Development*, 6(1), 13-19.

Zhumabaev, U.S. (2015). Concept of national security in the legislation of the Kyrgyz Republic: Problems and solutions. *Bulletin of the Kyrgyz-Russian Slavic University*, 15(5), 12-15.

Zhusuyeva, N.Zh. & Samatova, Zh.S. (2020). Information security in banks of Kyrgyzstan. *News of the Kyrgyz State Technical University named after I. Razzakov*, 53, 117-119.