Economic Affairs, Vol. **69**(Special Issue), pp. 33-42, February 2024
DOI: 10.46852/0424-2513.1.2024.5

AESSRA

Review Paper

The Impact of Cybercrime on State and Institutional Security: Analysis of Threats and Potential Protection Measures

Tetiana Baranovska[1*], Vladyslav Savitskyi[2], Mykola Serbov[3], Yurii Stoliar[4] and Yurii Krutik[1]

[1]Department of Law and Law Enforcement, Faculty of National Security, Law and International Relations, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
[2]Department of National Security, Public Management and Administration, Faculty of National Security, Law and International Relations, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
[3]Department of Public Administration and Environmental Management, Faculty of Computer Science, Management and Administration, Odesa State Environmental University, Odesa, Ukraine
[4]Department of Special Disciplines of the Law Enforcement Faculty, The Bohdan Khmelnytskyi National Academy of the State Border Service of Ukraine, Khmelnytskyi, Ukraine

*Corresponding author: tatyana_baranovs@ztu.edu.ua (**ORCID ID:** 0000-0002-6471-5932)

Received: 17-11-2023 **Revised:** 21-01-2024 **Accepted:** 02-02-2024

ABSTRACT

The article systematically reviews and analyses the phenomenon of cybercrime, with a focus on state and private cybercrime. The author highlights the main differences in characteristics, goals, resources, scale and consequences by comparing these phenomena. Real-life examples of cyberattacks are used to illustrate the diversity and threat of this issue to modern society. The second part of the article discusses measures to protect against cyberattacks, emphasising the main strategies at the state and private entity level. It highlights the importance of developing cybersecurity strategies, monitoring and response, cyber states of emergency, international cooperation, and intellectual property protection. The final section discusses the relevance of protecting against cyber threats and implementing measures to counteract this phenomenon in the context of the rapid development of cybercrime. It is noted that international cooperation, the development of standards and norms, and joint defence against cyber threats are key aspects of successfully countering state-sponsored cybercrime. It should be mentioned that the prevention and mitigation of cybercrime has become a crucial responsibility for all contemporary societies. This requires not only the implementation of technical security measures but also global collaboration between states and private sector entities, as well as the development of international strategies. The study confirms the significant impact of cybercrime on the security of states and institutions, particularly the increasing number of systematic attacks on critical infrastructure. It has been found that this phenomenon is becoming a global issue, necessitating effective international cooperation and the establishment of standards for the legal regulation of cyber activities. The findings emphasise the demand for all-encompassing approaches and actions to guarantee sustainable cybersecurity on both a national and global scale. The article discusses the increasing danger of state-sponsored cybercrime and the significance of creating defence strategies for states and institutions. The study analyses the distinctions between state and conventional cybercrime, identifies potential hazards, and recommends security measures. It also emphasises the necessity of international cooperation and the establishment of standards to effectively address this crucial issue.

HIGHLIGHTS

- Cybercrime, with its multifaceted manifestations ranging from hacking to cyberterrorism, poses a serious and evolving threat to the security of nations and institutions, necessitating a

How to cite this article: Baranovska, T., Savitskyi, V., Serbov, M., Stoliar, Y. and Krutik, Y. (2024). The Impact of Cybercrime on State and Institutional Security: Analysis of Threats and Potential Protection Measures. *Econ. Aff.*, **69**(Special Issue): 33-42.

Source of Support: None; **Conflict of Interest:** None

comprehensive approach that combines technical solutions, legal measures, and international cooperation.

- State-sponsored cybercrime, exemplified by recent incidents such as attacks on critical infrastructure and government agencies, presents a distinctive challenge requiring global collaboration, the establishment of common norms in cyberspace, and coordinated efforts to investigate and counteract cyber threats.

Keywords: Cybercrime, state security, cyberthreats, cybersecurity, international cooperation, information protection, security strategies, cyberattacks, cyberterrorism, propaganda

In the modern world, where information technology is an integral part of daily life, cybercrime presents new challenges. The growth of digital interaction and dependence on the internet has led to an increase in cyber threats that pose a serious challenge to the security of states and their institutions.

Cybercrime is a pressing and complex problem in modern society, encompassing hacker attacks, phishing attempts, and targeted attacks on critical infrastructure. This article analyses the impact of cybercrime on the security of states and institutions, as well as potential measures to protect against this type of threat.

Cyber threats pose a risk to the privacy and economic stability of countries and are increasingly influencing new security strategies. In today's world, information technology is intertwined with every aspect of our lives. Therefore, cybersecurity is crucial for ensuring the stability and security of states and their institutions. As the number and complexity of cyber threats increase, it is important to consider the role of states as perpetrators of cybercrime. The Russian Federation is particularly notable for its active cyberwar against Ukraine. In this context, analysing the impact of cybercrime on national and international security has become an essential part of security strategies.

Literature Review

Research on cybercrime considers the contributions of various authors in the field of information security. Nataliya B.S. (2004) discusses aspects of hacking and cybercrime, while Esther R., Seema G., and Usha M.S. (2015) draw attention to the global problem of cybercrime. Gordon S. and Ford R. (2006) provide definitions and classifications of cybercrime. Jean-Loup R. (2022) explores the evolution of cybercrime communities. Brunner (2019) examines the challenges and opportunities for combating cybercrime at the state and local law enforcement levels. Pasculli (2020) highlights the global causes and state responsibility for cybercrime. Magutu, Ondimu, and Ipu (2011) investigate the effects of cybercrime on state security about the introduction of optical fibre in Kenya. Watney (2012) examines the prospects for regulating cybercrime at the global level. Dalla G.N. (2015) analyses the regulation of transnational cybercrime in the context of international relations and the post-Westphalian regulatory state. Brenner S.W. (2006) explores the jurisdictional aspects of cybercrime. Sarre, R., Lau, L., & Chang, Y. (2018) investigate current trends in cybercrime response.

The impact of cybercrime on the security of states and institutions has been the subject of numerous studies. Brunner (2019) analyses the challenges and opportunities for combating cybercrime at the state and local law enforcement levels. Pasculli (2020) examines the global causes and state responsibility for cybercrime. Magutu *et al.* (2011) investigate the effects of cybercrime on state security about the introduction of optical fibre in Kenya. Watney (2012) explores the prospects for regulating cybercrime at the global level. Dalla (2015) examines the regulation of transnational cybercrime in the context of international relations and the post-Westphalian regulatory state. Brenner (2006) explores the jurisdictional aspects of cybercrime. Sarre *et al.* (2018) analyse current trends in cybercrime response. Peretti & Slade (2014) focus on state-sponsored cybercrime. Broadhurst *et al.* (2013) consider the interaction between organisations and cybercrime. Blinderman and Din (2017) discuss improving the domestic deterrence frame for cybercrime hidden in sovereign shadows. Tabansky (2012) considers cybercrime a national security issue. Finally, Brenner and Clarke (2004) propose a distributed security system to prevent cybercrime.

The purpose of the study is to analyse the impact of cybercrime on the security of states and institutions.

It examines the threats posed by cyberattacks and proposes measures to ensure effective protection against them. Additionally, the study aims to identify the importance of international cooperation and the development of strategies to counter state-sponsored cybercrime.

RESULTS

When examining the current challenges in the field of cybersecurity, cybercrime emerges as a significant threat to states and their institutions. Cybercrime encompasses not only the commission of crimes through the use of information technology but also all aspects of attacks on computer systems, networks, and electronic devices.

The range of cybercrime is broadening from conventional hacking and viruses to more intricate forms, including cyberespionage, cyberterrorism, and state cyber threats (Nataliya, 2004). Cybercriminals may be individual hackers, criminal groups, or actors operating at the state level.

A crucial aspect of cybercrime is the continuous development and enhancement of attack methods. As technology becomes more integrated into our daily lives and the functioning of states, cybercriminals are constantly adapting their strategies to new technological advances and finding new, highly sophisticated methods of penetrating information systems (Esther *et al.* 2015).

As technology continues to play an increasingly integral role in our daily lives and the functioning of states, cybercrime is becoming a more serious challenge to national security and stability. In this article, we will examine specific aspects of this problem and explore measures to effectively protect against cyber threats.

In our view, there are several definitions of cybercrime today:

1. Cyberspace crime refers to criminal acts committed using information technology and the Internet. This includes criminal acts that occur in the electronic environment, such as computer networks, online platforms, and electronic devices. Cybercrime encompasses a range of attacks, from hacking and viruses to more complex forms such as cyberterrorism and cyberespionage.

In this context, criminals use technology to illegally access information, commit economic crimes, and attack critical infrastructure. Cyberspace is increasingly becoming a platform for various criminal activities, as modern technologies play a crucial role in many areas of life, from business to public security (Gordon and Ford, 2006).

Criminals operating in this environment can commit identity theft, distribute malware, and disrupt the operation of government agencies or businesses. It is crucial to consider the continuous evolution and refinement of cybercrime techniques, as criminals are constantly adapting their methods to new technological challenges.

The approach to cybercrime considers the significance of information protection and cybersecurity for the efficient functioning of modern society and the economy. Preventing and combating this type of crime requires the interaction of technical, legal and international measures to ensure security in the electronic environment.

2. Internet-based crime is a type of cybercrime that involves using the Internet to commit offences. This encompasses a broad range of crimes that can be committed online, such as computer system attacks, phishing, online fraud, and other forms of electronic crime (Debarati and Jaishankar, 2011).

In the contemporary world, where the majority of business, communication, and transactions occur online, criminals are exploiting this opportunity to carry out various attacks. These may include theft of financial information, intrusion into corporate networks, and other forms of cybercrime.

Defending against internet-based crimes requires advanced methods due to the fast and sophisticated techniques employed by criminals. Furthermore, this approach compels society and legislators to respond proactively to changes in cyber defence and create new legal instruments to counter these challenges.

It is crucial to consider that criminals can operate on a global scale through the Internet, making these types of crimes challenging to detect and prosecute. Nevertheless, the advancement of security technologies and international cooperation plays a vital role in ensuring cybersecurity.

3. Electronic crime is a form of cybercrime that focuses on the technological aspects used to commit crimes. This includes the use of computer systems, software, and networks to commit various

crimes such as theft of confidential information, financial fraud, and the creation and distribution of malicious software (Peretti and Slade, 2014). Criminals use technological tools such as viruses, Trojans, ransomware, and other types of malware to commit crimes.

The rapid and continuous development of technology provides criminals with new opportunities, making it difficult to protect against electronic crime. Therefore, security measures should respond to the latest threats and attacks, considering the dynamics of technological progress.

It is crucial to comprehend that e-crime can be a worldwide occurrence, with criminals exploiting technology to perpetrate crimes on a global level. Therefore, international coordination and cooperation are indispensable to combat this form of cybercrime effectively.

4. Cyberfraud is a type of cybercrime that involves using technology to commit fraud. The use of internet resources, social media, email, and other electronic means to mislead people and obtain illegal benefits is also considered cyberfraud.

It can take many forms, including phishing attacks, where criminals impersonate trusted individuals or organizations to obtain confidential information. Other forms of cyber fraud include online fraud, where criminals use the internet to defraud individuals of their financial or personal information. This type of fraud is becoming increasingly prevalent in today's world, where most communications and transactions occur electronically. Fraudsters employ social engineering and deception techniques to deceive individuals and gain access to their personal or financial resources (Broadhurst *et al.* 2013).

Protecting against cyber fraud requires technical measures such as advanced fraud filtering and detection systems, as well as education and awareness-raising of the public about potential risks and methods of protection.

5. Cyberterrorism is the use of cyber tools to commit terrorist acts or interfere with state structures. This approach to cybercrime emphasizes the use of information technology to harm national security, the economy, or other strategically important objects (Tabansky, 2012).

Cyberterrorists can attack critical infrastructure facilities such as power plants, banks, and transport systems, or conduct attacks on communication and control systems. This form of cybercrime can have serious consequences for national security and stability. It is difficult to detect and counter due to the global nature of the Internet and the involvement of state agents or groups operating in other jurisdictions. Combating this type of cybercrime requires international cooperation, the development of modern cyber defence strategies, and the strengthening of security services' capabilities.

6. Information security involves protecting information from unlawful access, alteration, or deletion, with a focus on ensuring confidentiality, integrity, and availability in the face of increasing cybercrime threats (Brenner and Clarke, 2004).

These techniques include leaking sensitive data, attacking servers, or altering important information. Therefore, much attention is paid to developing and implementing effective encryption, authentication, and intrusion detection systems to ensure information security.

In today's world, where data is exchanged and stored digitally, criminals can use various techniques to harm organisations or states. Furthermore, as cloud computing expands and more devices connect to the internet, the significance of information security is increasing.

Effectively combating cybercrime within the realm of information security necessitates a blend of technical solutions, employee education, and the implementation of contemporary security standards.

Cybercrime is a form of criminal activity that utilises information technology to commit various types of crimes. It encompasses a wide range of activities, from relatively simple cases of online fraud to sophisticated cyber-attacks on corporate networks or even government systems.

In our opinion, the characteristic features of cybercrime are:

1. Cybercriminals can use various methods to illegally enter computer systems, steal confidential information or cause damage to systems.
2. A wide range of online frauds, including phishing, deception, financial data theft and bank account skimming, etc.

3. The use of cyber tools for espionage operations, including obtaining confidential information and hacking systems.
4. Use of information technologies to commit terrorist acts, attacks on critical infrastructure and influence political or social processes.
5. Sending or concealing viruses, DDoS (distributed denial of service) attacks to block network resources and cause damage to the network.
6. Using online resources to spread disinformation, influence public opinion and manipulate information.

The forms of cybercrime include:

1. Suspicious access to computer systems, networks and databases without appropriate authorisation.
2. Excessive sending or receiving of data, unexpected traffic that indicates uncertain or malicious activity.
3. Changes in the configuration of files, programs or system parameters without the user's knowledge.
4. Sending fake messages or emails from fake sources to obtain confidential information (phishing).
5. Attackers can exploit vulnerabilities in software or operating systems to gain unauthorised access.
6. Attempts to illegally gather intelligence through intrusions into computer systems.
7. Actions or negligence of the company's employees that may create internal security threats.
8. Spreading malicious software (viruses, Trojan horses, ransomware) to damage systems or gain unauthorised access.
9. Active monitoring of user activity to obtain valuable information.

Thus, cybercrime poses a serious threat to the security of states and various institutions, as modern technologies are integrated into various spheres of life. This impact can be diverse and include the following aspects:

1. Cyberattacks on energy, transport, telecommunications and other critical infrastructure systems can lead to serious disruption and interruption of operations.
2. Financial crimes and attacks on financial institutions can lead to significant economic losses and a decline in confidence in the financial system.
3. Cyber-espionage can reveal confidential information that can be used for political or economic manipulation.
4. Information campaigns and cyber-propaganda can influence public opinion by distorting facts and causing disinformation.
5. Attacks on important institutions, including military systems, can pose a threat to national security.
6. Use of technology to follow individuals or leak confidential information.
7. Attacks on voting systems, political platforms, and the spread of disinformation can affect political processes and election campaigns (Andini *et al.* 2023).

In the context of the war on the territory of Ukraine brought by the Russian Federation, the main challenges include enemy propaganda as a type of cybercrime (Geissler *et al.* 2023).

Propaganda is a tool commonly used to shape public opinion, influence beliefs, and create a favourable image for certain ideas or actions. In the digital era, propaganda has taken on new forms and opportunities due to the internet and social media.

1. Digital propaganda refers to the use of digital tools and internet technologies to influence public opinion, shape specific views, and manipulate information. These tools include social media, websites, blogs, news platforms, and other online resources (Guess *et al.* 2020).

In today's world, where most communication and information is done electronically, digital propaganda has become a powerful tool of influence. Digital propaganda can take many forms, such as the creation and dissemination of fake news, manipulation of images and videos, and the use of social media to distribute specific content on a large scale.

It provides an opportunity for microtargeting, where analytics and algorithms direct content to specific audiences.

The ongoing advancement of digital technologies has made digital propaganda more accessible and effective for a range of actors, such as government agencies, political organizations, and other social groups. This type of influence can have significant consequences for society, including its impact on democracy and information security.

The battle against digital propaganda necessitates a comprehensive approach that encompasses the creation of technical tools to identify and filter manipulative information, educational programmes to enhance media literacy, and the establishment of ethical standards for content producers.

2. Disinformation refers to the systematic dissemination of false, distorted, or manipulated information with the intention of misleading and influencing public opinion. In today's digital world, this type of influence has become particularly significant as information can spread rapidly through social media and other online platforms (Cole, 2022).

Disinformation can take various forms, but they all aim to create a distorted image of events or situations. It encompasses a range of tactics, including fake news, online forum attacks, and manipulated media.

Disinformation has the potential to impact public thinking, opinions, and even political decision-making. When disinformation becomes widespread, it can cause significant divisions in society and undermine trust in information sources.

Combating disinformation requires a combination of efforts from government agencies, civil society, and technical experts. Improving the media literacy of citizens, developing technical tools to detect disinformation, and supporting independent journalism are important components of such a strategy.

3. Algorithmic propaganda utilises social network and online platform algorithms to personalise and target content to specific audiences with the aim of influencing their beliefs and views. This phenomenon is analysed in the context of forming an individualised user experience with online platforms (Yeboah-Ofori *et al.* 2023).

Social media algorithms, such as those used by Facebook, Twitter, or YouTube, analyse vast amounts of data about users, including their views, likes, comments, and other interactions. Based on this data, the algorithms create a personalised stream of content for each user, directing them to what may be of interest.

However, this approach can have negative consequences. Algorithms can create 'filtered data', where users only engage with content that aligns with their own views and lose the ability to see a diversity of perspectives.

Additionally, personalised advertising can be achieved through algorithms, tailoring advertising messages to the interests and characteristics of each individual user. This raises concerns about data transparency and privacy.

Algorithmic propaganda requires attention to how algorithms determine what information users see and how this may influence their worldview. It is important to consider the ethical aspects of using algorithms in this context and develop strategies to create more diverse and objective information flows for users (Chaudhari *et al.* 2021).

4. Hybrid warfare is a multifaceted conflict strategy that employs a variety of tools to achieve strategic objectives. Information warfare is a crucial component of hybrid warfare, seeking to sway public opinion through disinformation and psychological tactics (Lock and Ludolph, 2020).

Economic pressure also plays a significant role in hybrid conflicts, where the use of economic sanctions and other measures can greatly impact the political decisions and behaviour of the adversary. Cyber-attacks are used to damage and paralyse computer systems and infrastructure.

Supporting local conflicts is another aspect of hybrid warfare. Encouraging or supporting force or unconventional means in internal conflicts can serve as a means of influencing the political situation in other countries.

Political manipulation plays a key role in hybrid warfare. The use of agents of influence, political groups or social movements to achieve political goals can generate instability and contribute to the achievement of strategic objectives.

Hybrid warfare involves the use of civilian, military, economic, information, and political instruments to achieve strategic objectives. To counter hybrid warfare, new strategies and approaches are required that challenge the current understanding of conflicts.

5. Viral propaganda is an influence strategy that aims to rapidly and massively disseminate information among a large audience (Pierri *et al.* 2023).

The primary objective of viral propaganda is to elicit an emotional response from the audience. Content and ideas that provoke strong emotions, such as amusement, admiration, or indignation, are frequently employed. This strategy helps to capture attention and make the information more memorable.

Another crucial element is the establishment of a community of consumers who actively share the content with their acquaintances, thereby contributing to its further dissemination. Creativity and originality also play a key role, as unconventional approaches attract attention and stimulate viral spread. Social media is an important channel for viral content, allowing information to be spread quickly and efficiently among users. However, this type of content can also be used to manipulate public opinion or trigger certain reactions among the audience (Pavlíková *et al.* 2021).

Viral propaganda can serve various purposes, such as advertising, political manipulation, entertainment, or social experimentation. To avoid potential negative impacts, it is crucial to develop critical thinking and awareness when consuming viral content (Fig. 1).

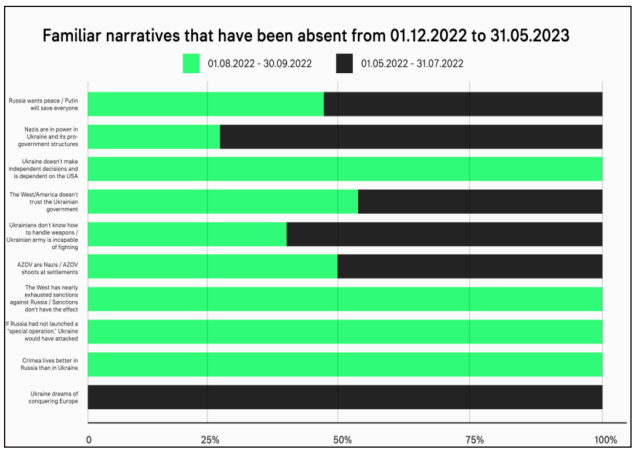

Fig. 1: Examples of the most popular expressions of Russian propaganda

When analysing the impact of cybercrime on state security, it is essential to remember that this problem is universal and affects all countries, regardless of their size or political status. In today's world, information technology plays a crucial role in driving development. Cybersecurity threats are widely recognised as they can affect international order and stability.

It is important to note that attempted and actual cyberattacks are not limited to individual states or regions. They can be planned and executed by various actors, including cybercriminals and cyber spies. States may also act as cybercrime actors, using these tools to achieve their strategic goals (Brunner, 2019).

The identification and prosecution of cybercriminals (agents, perpetrators of such attacks) is a significant challenge for the international community due to the global impact of attacks originating from various locations. When one state sanctions another, determining responsibility and identifying those who should be held accountable according to international law becomes a problem (Magutu *et al.* 2011; Blinderman *et al.* 2017).

After analysing these two similar phenomena, the main differences can be identified (Table 1).

State-sponsored cybercrime poses a threat not only to confidentiality and privacy but also to the fundamental principles of national security. The Russian Federation has been conducting serious attacks against Ukraine using various strategies, including hacker intrusions, disinformation campaigns, and cyber espionage.

This is a new challenge in today's world, where cyber threats have moved from isolated incidents to systematic, state-sponsored campaigns. Analysing and understanding the dynamics of state-sponsored cybercrime is crucial for developing effective protection and response strategies. Therefore, it is important to shed light on the role of states in the world of cybercrime.

We can also provide examples of cyberattacks and incidents that have occurred in recent years (Jean-Loup, 2022; Sarre et al., 2018) (Fig. 2):

1. In 2020, the SolarWinds software product was targeted by a group of hackers known as Cozy Bear or APT29. They inserted malicious code into patched software updates, resulting in a large-scale

Table 1: Characteristics and Comparison of State and Conventional Cybercrime

Characteristics	State-sponsored cybercrime	Common or private cybercrime
Sponsorship	Usually funded and supported by government agencies or intelligence services.	It can be financially motivated but is often not associated with state support.
Purpose	Usually aimed at political or military objectives, such as espionage, political influence, cyberterrorism.	Commonly has a financial goal, such as theft of confidential information, ransomware, or cyber fraud.
Resources	Has access to significant resources, including highly skilled cyber experts and advanced technology.	May use limited resources and may not always have access to numerous of specialists.
Scope	Can carry out large and complex operations with many participants.	Commonly smaller and less complex operations, focused on specific targets. Typically perpetrated by a single individual or group of individuals
International implications	It has the potential to cause serious international conflicts and tensions between countries.	Usually has a limited impact on international relations, although it can cause problems for individual organisations or countries.
Legality	Actions can be officially supported and legalised by state bodies or officials.	Usually illegal, violating national laws and international conventions.
Anonymity	Can use anonymous components, but may disclose its activities if it considers it strategically important.	Commonly involves greater anonymity, as actions are focused on the sale of criminal services or personal gain.
International Comprehensiveness	Ability to influence international politics and economics through cybercrime.	Commonly has limited international impact and is limited to private cases, local or regional aspects.

Source: *Magutu et al. 2011; Blinderman et al. 2017).*

incident that allowed the attackers to gain access to thousands of computers in government agencies and private companies.

2. In 2021, the Colonial Pipeline was targeted. The DarkSide group of attackers carried out a cyberattack on Colonial Pipeline, the largest fuel transportation pipeline in the United States. The attackers demanded a ransom and temporarily shut down the pipeline, causing problems with fuel supplies.

3. In 2021, JBS, one of the world's largest meat producers, was attacked by the REvil group, also known as Sodinokibi. Several meat processing plants were suspended, and ransom demands were made.

4. In 2021, the Microsoft Exchange service was attacked by cybercriminals representing the Chinese Hafnium group, who exploited vulnerabilities in servers. This attack resulted in the compromise of thousands of email systems.

5. In 2021, Kaseya, an IT infrastructure management software provider, was attacked by REvil. Through a software update, the attackers exploited a security vulnerability to compromise tens of thousands of computers.

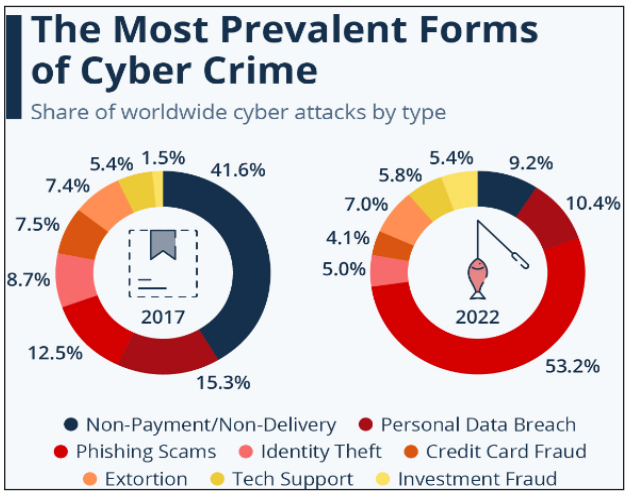

Fig. 2: Most popular forms of the cyber-crimes

These examples demonstrate the diversity of cybercrime recently, including attacks on government agencies, critical infrastructure, and private companies.

Measures to protect against cyberattacks see Table 2.

Table 2: Characteristics and Comparison of Measures to Protect Against State and Ordinary Cybercrime

Characteristics of the protective measure	State Cyber Threats	Private Cyber Threats
Developing cyber security strategies and policies	Development and implementation of comprehensive cybersecurity strategies at the state level.	Coordination and implementation of security policies at the organisational and company level.
Monitoring and response	Systems for monitoring and responding to cyber threats at the level of national infrastructures.	Use of monitoring and response systems at the corporate level.
Cyber emergency management	The use of special legal regimes, such as a cyber state of emergency, to effectively manage and coordinate crisis response.	Preparing and practising cyber-attack recovery plans to ensure rapid resumption of operations.
International cooperation	Participation in international forums and exchange of information to jointly counter cyber threats.	Entering into agreements and cooperation with other companies to share information and protect against threats.
Intellectual property and development	Protecting critical infrastructure and intellectual property from theft and cyber espionage.	Protecting confidential information, developments and patents from cyber fraud and theft.
Cyber hygiene of users	Developing and conducting campaigns to improve cyber hygiene among citizens.	Training and emphasis on IT security for company employees.
Regular updating and auditing of systems	Regular software updates and security audits.	Continuously updating systems and software, as well as audits to identify weaknesses.
Protection of personal information	Strict control over the processing and storage of citizens' personal data.	Ensuring a high level of protection of customer personal data and corporate information assets.

Source: *Watney, 2012; Dalla, 2015; Brenner, 2006.*

DISCUSSION

Ensuring cybersecurity protection is becoming an important task for states and institutions in a world where cybercrime is rapidly evolving. Implementation of preventive protection measures, incident response and international cooperation is getting key to ensuring sustainable and effective protection against cyber threats.

When examining state-sponsored cybercrime, it is crucial to emphasise the significance of international cooperation and the creation of common counteraction strategies. It is important to note that state-sponsored cybercrime presents multifaceted challenges that necessitate the collaboration of all nations and international organisations.

A vital aspect is the establishment of global standards and norms that would define the regulations of cyberspace. Such agreements assist in establishing responsibility and determining legal consequences for states that carry out cyberattacks. International cooperation in investigating and suppressing cybercrime is becoming crucial to successfully combat this phenomenon.

Common defence against cyber threats involves exchanging information between countries and regions. Countermeasures must be carefully coordinated and tailored to the specifics of each situation. Effective counteraction to state-sponsored cybercrime requires cooperation between cyber police and law enforcement agencies from different countries (Pasculli, 2020).

CONCLUSION

Cybercrime is a type of crime that involves the use of information technology and cyberspace to commit offences. It can take various forms, such as hacking, phishing, cyberterrorism, electronic fraud, and others. Criminals can use these technologies to gain unlicenced access to data, cause damage, or even carry out terrorist attacks.

Signs of cybercrime include unauthorised access to systems, abnormal network activity, phishing attacks, exploitation of software vulnerabilities, cyber espionage, and malware. Cybercriminals

can use various methods, adapting them to new technological realities and challenges.

Cybercrime is a global challenge that can affect all areas of society and the economy. Preventing and combating cybercrime requires not only technical security measures but also the development of international standards, cooperation between countries, and the definition of responsibility for cyber activities.

It is critical to understand the different aspects of cybercrime and take measures to protect against it in today's society, where digital technologies are intertwined with all areas of life.

REFERENCES

Andini, N., Damayanti, N., Sari, N., Fkun, E. and Erkamim, M. 2023. Cybercrime and Threats to the Electoral System. *J. of Digital Law and Pol.*, **3**(1): 26-37.

Blinderman, E. and Din, M. 2017. Hidden by sovereign shadows: improving the domestic framework for deterring state-sponsored cybercrime. *Vand. J. Transnat'l L.*, **50**: 889.

Brenner, S.W. 2006. Cybercrime jurisdiction. *Crime, Law and Social Change*, **46**: 189-206. https://link.springer.com/article/10.1007/s10611-007-9063-7. Last Accessed date 18th January, 2023.

Brenner, S. W., Clarke, L.L. 2004. Distributed security: Preventing cybercrime. *J. Marshall J. Computer & Info. L.*, **23**: 659.

Broadhurst, R., Grabosky, P., Alazab, M. and Bouhours, B. 2013. Organizations and cybercrime. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2345525

Brunner, M. 2019. Challenges and opportunities in state and local cybercrime enforcement. *J. Nat'l Sec. L. & Pol'y*, **10**: 563. Last Accessed date 18th April, 2023.

Chaudhari, D.D. and Pawar, A.V. 2021. Propaganda analysis in social media: A bibliometric review. *Information Discovery and Delivery*, **49**(1): 57-70. Last Accessed date 17th November, 2023.

Cole, R. 2022. Encyclopaedia of propaganda. *Routledge*. https://books.google.com.ua/books?hl=uk&lr=&id=emVjEAAAQBAJ&oi=fnd&pg=PP1&dq=propaganda&ots=7f-KYRZ5AD&sig=NlUZSKBvIGyoHpgr3QHlgXK9C48&redir_esc=y#v=onepage&q=propaganda&f=false Last Accessed date 18th December,2023

Dalla, G.N. 2015. Governing the ungovernable: International relations, transnational cybercrime law, and the post-Westphalian regulatory state. *Transnational Legal Theory*, **6**(1): 211-249.

Debarati, H. and Jaishankar, K. 2011. *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations*. https://doi.org/10.4018/978-1-60960-830-9

Esther, R., Seema, G. and Usha, M.S. 2015. A Study on the Cyber-Crime and Cyber Criminals: A Global Problem. *Int. J. Computing Algorithm*, **4**(1): 7-11.

Geissler, D., Bär, D., Pröllochs, N. and Feuerriegel, S. 2023. Russian propaganda on social media during the 2022 invasion of Ukraine. *EPJ Data Science*, **12**(1): 35.

Gordon, S. and Ford, R. 2006. On the definition and classification of cybercrime. *J. Comput. Virol.*, **2**: 13–20.

Guess, A.M. and Lyons, B.A. 2020. Misinformation, disinformation, and online propaganda. *Social media and democracy: The state of the field, prospects for reform*, **10**.

Jean-Loup, R. 2022. How cybercriminal communities grow and change: An investigation of ad-fraud communities, *Technological Forecasting and Social Change*, **174**.

Lock, I. and Ludolph, R. 2020. Organizational propaganda on the Internet: A systematic review. *Public Relations Inquiry*, **9**(1): 103-127. Last Accessed date 28th May, 2023.

Magutu, P.O., Ondimu, G.M. and Ipu, C.J. 2011. Effects of cybercrime on state security: Types, impact and mitigations with the fiber optic deployment in Kenya. *J. Info Assurance & Cybersecurity*, (1): 1-20.

Nataliya, B.S. 2004. Hacking and cybercrime. In Proceedings of the 1st annual conference on Information security curriculum development (InfoSecCD '04). *Association for Computing Machinery*, New York, NY, USA, 128–132. https://doi.org/10.1145/1059524.1059553

Pasculli, L. 2020. The Global Causes of Cybercrime and State Responsibilities: Towards an Integrated Interdisciplinary Theory. *J. Ethics and Legal Technologies (JELT)*, **2**(1): 48-74.

Pavlíková, M., Šenkýřová, B. and Drmola, J. 2021. Propaganda and disinformation go online. *Challenging online propaganda and disinformation in the 21st century*, 43-74. Last Accessed date 18th January, 2023.

Peretti, K. and Slade, J. 2014. State-Sponsored Cybercrime: From Exploitation to Disruption to Destruction. *The SciTech Lawyer*, **10**(2). Last Accessed date 17th November, 2023.

Pierri, F., Luceri, L., Jindal, N. and Ferrara, E. 2023. Propaganda and Misinformation on Facebook and Twitter during the Russian Invasion of Ukraine. *In Proceedings of the 15th ACM Web Science Conference 2023*, 65-74. https://dl.acm.org/doi/abs/10.1145/3578503.3583597

Sarre, R., Lau, L. and Chang, Y. 2018. Responding to cybercrime: current trends. *Police Practice and Research*, **19**(6): 515-518.

Tabansky, L. 2012. Cybercrime: A national security issue? *Military and Strategic Affairs*, **4**(3): 117-136. Last Accessed date 25th January, 2023.

Watney, M. M. 2012. The way forward in addressing cybercrime regulation on a global level. *J Internet Technology and Secured Transactions (JITST)*, 1, 62-67.

Yeboah-Ofori, A., and Opoku-Boateng, F. A. 2023. Mitigating cybercrimes in an evolving organizational landscape. *Continuity & Resilience Review*, **5**(1): 53-78. Last Accessed date 5th October, 2023.