ECONOMIC CONSEQUENCES OF CYBERCRIME AND LEGAL REGULATION MECHANISMS IN GEORGIA

RESEARCH GROUP:
Tamar Makasarashvili-
Doctor of Economic Sciences, Professor,
Gori State Teaching University, Georgia

Tea Khorguashvili-
Doctor of Economic Sciences, Professor,
Gori State Teaching University, Georgia

Giuli Giguashvili-
Doctor of Economic Sciences, Professor,
Gori State Teaching University, Georgia

Aleksandre Sadagashvili-
Student of Bachelor’s Programme in Law,
Gori State Teaching University, Georgia

Summary. With the development of Internet technologies, cybercrime has also evolved and diversified. Much of the world’s economic and business information comes from electronic information, and the need for remote work caused by the coronavirus (COVID-19) pandemic has further increased demand for e-services, which in turn has contributed to increased technology risks, threats, and incidents. The main task of the states is to actively fight against the negative socio-economic, financial, and political consequences caused by the growth of cybercrime. The main purpose of the study is to assess the negative consequences of cybercrime in Georgia, the main threats to information security, to develop recommendations for the prevention of cybercrime, to improve its legal regulation mechanisms. The fight against cybercrime in Georgia is carried out using criminal norms. The law “On Information Security” is in force in the country, Georgia’s cyber security strategy has been developed, but this process needs constant development. The main task of the state is to gradually improve the legislation and bring it in line with modern technologies, to ensure close cooperation between the state and society, to raise the awareness of civil society. It is essential to constantly inform the public and companies about cyber threats, as effective prevention is the best form of crime prevention policy.

Keywords: Cybercrime, Information Security, Cyber Security Strategy, Cybercrime Regulation.

Introduction.
The 21st century is an era of globalization. The world is becoming more and more "open" to the processes taking place in different parts of the world, the virtual borders between countries are becoming weaker, which is related to the
computerization process, and in a way, it owes its merit. As in the rest of the world, the scale of internet coverage in Georgia has increased considerably. According to official statistics from the United Nations International Telecommunication Union (ITU), more than 70% of Georgia's population has access to the Internet. However, according to various internal e-readiness surveys, this figure reaches a much higher level: according to the National Statistics Office of Georgia (Geostat), it is almost 98% with companies. The issue of providing secure and secure cyberspace was put on the agenda to further develop the information society, to create a credible environment for e-commerce, information-communication technologies, and transactions, as well as e-government services in the public and private sectors.

The goal of research. Advances in technology have made the economic activity more efficient and affordable. It made it easier for companies to offer products and services to customers, negotiate and execute trade agreements. However, with the growing dependence on cyberspace, the threat of cybercrime has also increased. The world of criminals has easily adapted to virtual reality and with the use of new technologies, the negative socio-economic consequences of cybercrime have increased: Millions of funds have been misappropriated, huge amounts of criminally obtained money are being "revived", taxes are being evaded, and complex measures are being taken to prepare and carry out various cybercrimes. Specialists predict the rapid growth rate of organized crime using a computer. The main task of mankind is to actively fight against the negative consequences caused by the introduction of modern computer and Internet technologies.

Literature review. Cybercrime is the most pressing of computer crimes. Cybercrime is the second most common crime today, after drug and arms trafficking. [1] It refers to any crime that takes place in cyberspace.

Researchers distinguish between crimes against the Internet, databases, information technology systems, or their data (cybercrime in the narrow sense) and crimes committed using information or communication technologies (cybercrime in the broad sense). [2] Such crimes include hacking into other people’s computer systems, attacking and subsequently spreading cyberbullying, hacking credit card and e-mail passwords, obtaining, editing, and disseminating personal or state-of-the-art information; Attacks against critical infrastructures, and more.

Along with the public sector, business entities are increasingly being targeted by cyber-attacks to paralyze them and cause economic damage. For example, in 2016, a large-scale "DDoS" attack on the Georgian banking sector and public electronic financial services disrupted the operation of online banking services and the state tax system, causing significant economic damage to the sector. Attacks on critical infrastructures include phishing, ransomware, deface, DDoS, and mail spoofing. [3]

Cybercrime first came to the fore in the 1970s. The American Alphonse Confessor embezzled 602 thousand US dollars using an electric calculator and became the first cybercriminal in the history of world criminology. Following this fact, the study of this phenomenon at the national and international levels began. The United States enacted the Federal Computer Protection Act in 1977.

According to the Criminal Code of Georgia, an illegal act is considered a cybercrime, which includes at least one of the components listed in the provisions of Articles 284, 285, and 286 of the same Code and not any illegal act committed using a computer system. For example, unauthorized access to a computer system
(Article 284), illegal use of computer data and/or computer system (Article 285), encroachment on computer data and/or computer system (Article 286), encroachment on computer data, and/or computer system for financial gain (Article 2861), creation of fake official computer data (Article 2862), etc. [4]

In the main cases, there are several types of cybercrime: cyberbullying, cybervandalism, cyberbullying, cyber theft, cyberterrorism.

Depending on who or what the cybercrime can be directed against, there are three main categories:

- Crimes against the person;
- Property crimes;
- Crimes against the state.

The situation in Georgia is quite difficult in this regard. Georgia ranks first in terms of the distribution of unlicensed products. Most of the products uploaded on Georgian sites - movies, music, programs - are not licensed. As a rule, hackers either erase or change their traces, making it almost impossible to find and identify them. [5] A particular problem is the illegal acquisition and dissemination of personal information. The inviolability of a person's private life is guaranteed by the Constitution of Georgia and enshrined in several international legal acts. There is a serious protest in society on the issue of covert surveillance and privacy, and important measures have been taken by the authorities in this regard. Nevertheless, influencing people, especially women, and blackmailing them through their private life recordings through covert surveillance continues to be one of the most serious problems and challenges in our country. [6]

In many cases, the crime was committed using cyber methods from the territory of another country, which complicates both the process of obtaining evidence and the identification of the perpetrator. This is indicated by the fact that according to the Ministry of Internal Affairs [7], still in 2018, compared to the previous year, the number of cybercrime has doubled. According to statistics, 613 cases of this type of crime were detected, which is 111% more than in the same period of 2017. With the increase of these types of crimes, the rate of their opening has also decreased. In 2017, law enforcement uncovered 23% of cybercrime, and in 2018 that number reduced to 11.7%. Almost 90% of cybercrime remains unsolved. [8]

The number of convicts for computer crime has been increasing in recent years (Articles 284-286 of the Criminal Code). (Table # 1)

<table>
<thead>
<tr>
<th>Computer Crime (Articles 284-286 of the Criminal Code)</th>
<th>Initiation of criminal prosecution (number of persons)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article</td>
<td>2016</td>
</tr>
<tr>
<td>Intrusion into computer system without permission (Article 284)</td>
<td>87</td>
</tr>
<tr>
<td>Illegal use of computer data and/or computer system (Article 285)</td>
<td>4</td>
</tr>
<tr>
<td>Damaging computer data and/or computer system (Article 286)</td>
<td>20</td>
</tr>
</tbody>
</table>

Source: https://www.geostat.ge/ka/modules/categories/679/siskhils-samartlis-statistikis-ertiani-angarishi
To regulate cybercrime, the Law on Information Security was adopted in Georgia on June 19, 2012 [9], which sets general standards for information security. The purpose of the law is to facilitate the effective and efficient implementation of information security, to establish the rights and responsibilities of the public and private sectors in the field of information security, as well as to establish state control mechanisms for the implementation of information security policy.

According to the law, the priority threats to cyber security include:

A) a cyber-attack that threatens human life and health, state interests, or the country’s defense capabilities;
B) cyber-attack against critical information system subject information systems;
C) a cyber-attack that threatens the financial resources and/or property rights of a state, organization, or individual, etc.

Several reforms have been implemented in recent years:

• The Cybercrime Division has been established in the Central Criminal Police Department of the Ministry of Internal Affairs of Georgia, which is responsible for detecting, preventing, and preventing illegal acts committed in cyberspace;
• The Office of the State Inspector oversees the legality of personal data processing in the country and is responsible for enforcing data protection legislation;
• The National Bank of Georgia is authorized to establish additional standards and requirements for the commercial bank operating under its supervision to manage both information security policy and information assets;
• A computer-digital expertise subdivision has been established within the Forensic Main Division of the Ministry of Internal Affairs (MIA). Standard operating procedures for the primary handling of digital evidence have been developed. The documents define the types of software and technical rules according to which digital evidence should be processed;
• The Academy of the Ministry of Internal Affairs (MIA) has developed special training modules that cover the following issues related to cybercrime: electronic evidence searches, cybercrime investigative equipment, legal aspects of cybercrime, etc.

Based on the analysis of the threats and challenges identified in the fight against cybercrime, the legal framework is constantly updated, material and technical capabilities are developed, and international police cooperation is deepened at the operational and non-operational levels. Also, various measures are being taken to raise public awareness about cybercrime and the damage caused by it.

It should be noted that the Georgian National Cyber Security Strategy, which is the main document defining the state policy in the field of cyber security, was initially developed for 2013-2015, later, the National Cyber Security Strategy for 2017-2018 was adopted, and on September 30, the Government of Georgia №482 Approved the National Cyber Security Strategy of Georgia 2021 - 2024 and its action plan. [3]

The third strategy reflects the changes that have taken place in the country’s cybersecurity environment since the adoption of previous strategies, and sets out a vision for the safe development of the country over the next three years, defining effective mechanisms to deal with threats and challenges. The main goals of the 2021-2024 strategy are: to develop the cyberculture of information societies and organizations and to strengthen their capacity to deal with threats and incidents in
SECTION X

VI. INFORMATION TECHNOLOGIES AND SYSTEMS

cyberspace; Strengthening the cyber security management system and strengthening public-private partnerships; Development of cyber capabilities with strong human resources and appropriate technical means, strengthening the role of Georgia as a safe and secure country in the international arena of cyber security.

Also important are national security strategies, which include a cyber security component: the Georgian National Strategy for Combating Terrorism, the National Strategy for Combating Organized Crime, the Georgian Foreign Policy Strategy, and others. [3]

Research Results. Due to the irreversible technological progress in the modern world, the growing dependence of society and business on the media, the transition to the digital economy, the growing threat of cybercrime. At the same time, the growing reliance on e-services caused by the coronavirus (COVID-19) pandemic, the large-scale introduction of appropriate systems to ensure remote operation, poses additional security challenges. The development of artificial intelligence has its an impact on the security of cyberspace.

Given the above, it is necessary to improve the legal framework, further develop the material and technical base of the agencies involved in the fight against cybercrime, and raise the professional level of the staff. The state needs to strengthen the security of critical infrastructure and information systems and the ability to detect and combat cybercrime. Unfortunately, in terms of cybersecurity development, Georgia has lost its leading position in recent years - if in 2018, it was considered a leader in the region among the countries of the South Caucasus and the Black Sea basin, as confirmed by the International Telecommunication Union (ITU) Global Cyber Security Index (GCI) (According to the results of 2018, Georgia ranked 18th in the world and 9th in Europe), in the 2020 Global Cyber Security Index, Georgia ranked 55th with 81.06 points, down several tens from previous years, and only 30th in the European region. [10] Georgia's deteriorating position, along with the pandemic, can be explained by the delay in technological progress.

We think that the best mechanism to fight cybercrime is close cooperation between the state and society. Citizens need to know how to protect themselves from cybercrime, they need to be aware of potential threats, identify them and respond to them. Given this, it is important to update the legal framework for combating cybercrime, taking into account international best practices and practices; Increase public awareness; Ensuring the secure implementation of electronic transactions and promoting the smooth development of the economy and business in the country; Strengthening international cooperation, which remains a challenge for the state.

Conclusions and suggestions. In conclusion, it can be difficult to accurately predict the changes and measures taken concerning cybercrime to be effective and efficient. It is desirable to raise public awareness about the dangers of cybercrime and to develop some kind of defense mechanism. It would be advisable to start studying the rules of safe use of the Internet in schools. We think it is necessary to take into account the recommendations that experts recommend for protection against cybercrime: do not use unlicensed programs; do not post mail to strangers; do not open questionable sites; do not use the computer without a security system. Do not open and reply to emails from
unknown addresses. Do not follow the links posted on various websites that promise to make you money. Do not assign your bank account number and PIN code to anyone. Verify any information we receive electronically, even if it comes from a friend's address. The internet is boundless space, through it we can connect with people anywhere in the world in one second. The threat posed by this global network is real. We decide to heed the recommendations of the world and protect ourselves from crime if we become victims of cybercriminals.

References: