

# Cybercrime in Georgia: Current Challenges and Possible Developments

# **Cybercrime in Georgia: Current Challenges and Possible Developments**

*Authors: **Nata Goderdzishvili, Shalva Khutsishvili***

*Reviewer: **Giorgi Khishtovani***

*Research Assistant: **Giorgi Tsulaia***

# CONTENTS

<b>Abbreviations</b> .....	2
<b>Chapter I. Introduction</b> .....	3
1. Background .....	3
2. Scope of the Work .....	5
3. Methodology .....	5
<b>Chapter II. Mapping Georgia`s Cybercrime Landscape</b> .....	6
1. Understanding of Cybercrime .....	6
2. Main Cybercrime Threats .....	7
3. Cybercrime Statistics .....	14
4. Cyber Incidents Statistics .....	17
5. Main Threat Actors .....	19
<b>Chapter III. Cybercrime and the National Security</b> .....	22
<b>Chapter IV. Trends in the Neighborhood</b> .....	27
1. Azerbaijan .....	27
2. Armenia .....	28
3. Russian Federation .....	28
4. Ukraine .....	30
5. European Union .....	31
6. Lithuania .....	32
<b>Chapter V. Georgia's handling of cybercrimes and its challenges</b> .....	33
1. Institutional, policy and legislative frameworks .....	34
2. Capacity and Resources (workforce, technical equipment) .....	36
3. Cybercrime Reporting, Classification and Information Sharing .....	38
4. Public Awareness and Social Engagement .....	39
<b>Chapter VI. Key Findings and Recommendations</b> .....	41
1. Key Findings .....	41
2. Recommendations .....	42
<b>Chapter VII. Conclusion</b> .....	45

## ABBREVIATIONS

<b>BEC</b>	– Business Email Compromise BEC
<b>CCPD</b>	– Central Criminal Police Department of the Ministry of Internal Affairs of Georgia
<b>CCG</b>	– Criminal Code of Georgia
<b>CERT</b>	– Computer Emergency Response Team
<b>CIs</b>	– Critical Infrastructures
<b>CIS</b>	– Commonwealth of Independent States
<b>DGA</b>	– Digital Governance Agency
<b>DEA</b>	– Data Exchange Agency
<b>EaP</b>	– Eastern Partnership of the European Union
<b>ENISA</b>	– European Union Agency for Network and Information Security
<b>EU</b>	– European Union
<b>Europol</b>	– European Union Agency for Law Enforcement Cooperation
<b>FBI</b>	– Federal Bureau of Investigation
<b>FOI</b>	– Freedom of Information
<b>GCI</b>	– Global Cybersecurity Index
<b>GDPR</b>	– General Data Protection Regulation 2016/679 of the European Parliament and of the Council
<b>GOG</b>	– Government of Georgia
<b>GOCG</b>	– Georgian Organised Crime Groups
<b>ICT</b>	– Information Communication Technologies
<b>Interpol</b>	– International Criminal Police Organization
<b>ISP</b>	– Internet Service Provider
<b>ITU</b>	– International Telecommunication Union
<b>LEA</b>	– Law Enforcement Authority
<b>LEPL</b>	– Legal Entity of Public Law
<b>MFA</b>	– Ministry of Foreign Affairs
<b>MIA</b>	– Ministry of Internal Affairs
<b>NCS</b>	– National Cybersecurity Strategy
<b>NIS</b>	– Network and Information Systems Directive
<b>OCSA</b>	– Online Child Sexual Abuse
<b>STEM</b>	– Science, Technology, Engineering, and Mathematics
<b>SSSG</b>	– State Security Service of Georgia

# CHAPTER I. INTRODUCTION

## 1. Background

Digital transformation created a new virtual (cyber) sphere for social relations - parallel to the physical one. Approximately one-third of the world's population has access to the internet and takes part in different activities offered by the virtual sphere.<sup>1</sup> The evolution of cybersphere facilitated simplification and intensification of transnational economic and social relations, and at the same time opened new opportunities for illegal activities. With the technological revolution, information flow has been simplified, but information protection and data security have become more difficult. Cybercrimes emerged as the consequent characteristic of the ICT-enabled ecosystem.<sup>2</sup> One can hardly find any national or international strategic documents or policy analysis of criminal threats without significant stress on increased cybercrime challenges. 80-90% of crimes committed globally have elements of cybercrime. Also, technological sophistication of the threat environment is being dramatically developed.<sup>3</sup>

Georgia faced the first major challenge in cybersphere during the 2008 Russia-Georgia war, when the country having limited capacity in this domain, suffered a massive cyberattack.<sup>4</sup> Since then, the Government of Georgia (GOG) has implemented important institutional<sup>5</sup>, legal<sup>6</sup> and policy<sup>7</sup> reforms in order to strengthen security, safety and resilience of its cyberspace.

---

<sup>1</sup> See, *Anatomy of Hybrid Wars*, edited by Tinatin Khidasheli, Tbilisi, 2020; pp. 365.

<sup>2</sup> 1966 bank hacking in Minneapolis, Minnesota by computer programmer is considered the first official cyber case. Other more famous cybercrime conviction is hacking of AT&T network in 1981 and later in 1973, when embezzlement of 2 million USD from Citibank was taken place in New York through using computer by bank teller (<https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/>). Lawrence M. Salinger. *Encyclopaedia of White-Collar and Corporate Crime*, Vol. 1. SAGE Publications. 2005. p. 191.

<sup>3</sup> Council of Europe presentation during Moldova Cyber Week 2020 <https://moldovacyberweek.md/>

<sup>4</sup> <https://www.nytimes.com/2008/08/13/technology/13cyber.html>

<sup>5</sup> Data Exchange Agency (DEA) under the Ministry of Justice in 2010 and Cybersecurity Bureau under the Ministry of Defence in 2013 were established mandated to handle cybersecurity incidents and threats in civilian and military spheres respectively. Cybercrime Division of CCPD at the Ministry of Internal Affairs (MIA) was created in 2012 to investigate cybercrimes.

<sup>6</sup> Georgian law on Information Security adopted, cybercrimes criminalized by Criminal Code of Georgia, approval of the Budapest Convention in 2012. Relevant documents available at: [www.matsne.gov.ge](http://www.matsne.gov.ge)

<sup>7</sup> Approval of two successive national cybersecurity strategies, e-Georgia strategic vision, launching of large scale e-government systems [www.matsne.gov.ge](http://www.matsne.gov.ge); <https://idfi.ge/en/e-governance-e-participation-georgia-index-2020>; <https://eni-seis.eionet.europa.eu/east/areas-of-work/communication/events/project-related-events/open-data-and-e-governance-for-environment-national-roundtable-in-georgia/presentations/4.%20Digital%20Georgia%20-%20EN.pdf>

Comprehensive reforms made Georgia ranked the 8th in 2017 Global Cybersecurity Index (GCI)<sup>8</sup> and the 18<sup>th</sup> in its 2018 ranking.<sup>9</sup> Implementation of e-government program and digitalisation of public services<sup>10</sup> triggered a boost of ICTs in the Georgian public and private sectors with a consequent side effect - a significant increase of cybercrime statistics in recent years.<sup>11</sup> The latest statement of the Minister of Internal Affairs of Georgia, Vakhtang Gomelauri identified about 24% rise in cybercrime rate in January-November of 2020 in the light of 10% decrease in Georgia's total registered criminal cases in comparison with the previous year.<sup>12</sup>

Security in cyberspace becomes even more crucial for contemporary Georgia as the country faces serious hybrid threats<sup>13</sup> often realised in practice through technological means. Aside from the geopolitical discourse and hybrid warfare, there is also another alarming factor that exacerbates this issue - increasing utilization of technologies by transnational criminal groups that pose a serious challenge for the international community Georgia is a part of. Georgian organised crime groups (GOCGs) are actively involved in transnational criminal activities.<sup>14</sup> What is more, transnational crime has been in the focus of Georgian society more actively since the beginning of the EU-Georgian Association process and visa liberalisation agenda. These determinants, in addition to traditional criminal justice aspects, emphasize the importance of cybercrime as a problem of public interest.

Despite the boost of digitalisation, public awareness of cybercrime or cybersecurity risks and threats is relatively low in the country. Georgian society is mostly irresponsive and unprepared towards cyber threats, while the Georgian private sector is absolutely free from regulatory standards in this domain that plays a certain role in limited social activism in the process of building cyber resilience.<sup>15</sup>

No large-scale government-sponsored public cyber awareness campaigns were reported in recent years. In addition, the media coverage only scratches the surface of the problems; cases of the in-depth analysis regarding cybercrime or major cybersecurity

---

<sup>8</sup> [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf)

<sup>9</sup> [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf)

<sup>10</sup> Statistics from Digital Governance Agency (DGA): number of e-services offered through [www.mygov.ge](http://www.mygov.ge) amounts to 700 in 2020 compared to 30 in 2012, there are up to 250, 000 users registered on [mygov.ge](http://mygov.ge) with new 100, 000 registered individuals just in 2019.

<sup>11</sup> <https://police.ge/ge/useful-information/statistics>

<sup>12</sup> <https://www.agenda.ge/en/news/2020/3953>

<sup>13</sup> Anatomy of Hybrid Wars, edited by Tinatin Khidasheli, Tbilisi, 2020; pp. 91-105;

<sup>14</sup> 2017-2020 Georgia's National Strategy on Combatting Organised Crime, available at: <https://info.police.ge/uploads/5f3fa36969432.pdf>

<sup>15</sup> The E-Readiness survey respondents stated that only to the half of them security and privacy was important and they paid attention to it, while less than 30% used any cybersecurity tools and solutions as such. E-Readiness study implemented by IPM in 2016 initiated by USAID/Tetra Tech ARD, in frames of E-Georgia Project.

incidents are also rare in Georgian media. Cybercrime is quite a new research topic in Georgian reality and there are a few studies about it, even relevant government agencies do limited work in cybercrime research domain. The Georgian Police remain relatively transparent regarding cybercrime statistics but rarely go into public discussions about causes, trends and other details.

The goal of this research is twofold. Primarily, it provides an assessment of the cybercrime situation in Georgia and projection of possible developments, as well as envisages policy recommendations for responsible public authorities. The secondary, but not less important goal is to facilitate awareness-raising through developing analytical information regarding problems and ways of their solutions. Georgian citizens are end victims who suffer from any national security threats including cybersecurity incidents and cybercrimes. Informing the public and raising awareness gain utmost importance, especially in conditions of hybrid threats. Social resilience could not be ensured without a wider engagement of informed and socially active citizenry.<sup>16</sup>

## **2. Scope of the Work**

The research yields analysis of the state of play of the cybercrime and cyber incident, trends and challenges in Georgia. It describes Georgia's current cybercrime ecosystem, key threat dimensions and emerging cybercrime reality in a wider context of international trends and developments. This paper also explores Georgia's approach to cybercrime reporting, threats and incidents knowledge sharing as important instruments for evidence-based policy making. Finally, the research paper comes up with key conclusions and provides the best possible policy recommendations for combating cybercrime.

## **3. Methodology**

Collection of data was conducted through desk research from primary sources: official policies, strategies, reports and secondary sources: analytical documents, academic research, surveys and other available information. The statistical data published by the Ministry of Internal Affairs (MIA), relevant regional and international institutions and their threat assessments were explored as important sources. For the purpose of the desk research, Freedom of Information (FOI) was requested from the MIA, LEPL Digital Governance Agency, and General Prosecutor's Office of Georgia. Besides the desk research, the interviews with the representatives of government institutions and independent experts were conducted.

---

<sup>16</sup> UNDERSTANDING CYBERCRIME: Phenomena, Challenges and Legal Response – [www.itu.int](http://www.itu.int)

# CHAPTER II. MAPPING GEORGIA'S CYBERCRIME LANDSCAPE

## 1. Understanding of Cybercrime

Cybercrime is a broad term and describes criminal activity committed on the internet<sup>17</sup> or in the wider sense in cyberspace. Cybercrime can be categorized as cyber-dependent and cyber-enabled. Cybercrime is cyber-dependent, when it can only be committed using a computer, computer networks or another form of information technology (for example ransomware).<sup>18</sup> There are also cyber-enabled criminal activities when traditional crime conducted in offline environments (e.g., fraud, theft) is committed by using ICTs to make its perpetration easy, successful or to increase its scale.<sup>19</sup> Traditionally, pure cybercrimes are those which target the security, integrity, confidentiality or availability of data or software stored on computer systems or networks. The MIA usually calculates cybercrime statistics on the bases of registered cyber-dependent crimes.<sup>20</sup>

The main targets of cybercrime can generally be divided into three categories: 1. Cybercrimes against persons; 2. Cybercrimes against property; 3. Cybercrimes against the government. This classification includes the following offences: Denial-of-service attacks, cracking, child pornography, espionage, financial theft, drug trafficking, fraud, etc.<sup>21</sup> One of the features of cybercrime that makes it very distinctive from another type of crime is that it can be committed by state actors.<sup>22</sup> It creates an excellent opportunity for external threats to be transformed into serious internal problems of any country (e.g., attacks on the Saudi Aramco oil company<sup>23</sup>, Ukraine's health and energy sector<sup>24</sup>, 2020 the US government data breach<sup>25</sup>, etc.). This aspect of the problem will be discussed in Chapter III.

---

<sup>17</sup> UNDERSTANDING CYBERCRIME: Phenomena, Challenges and Legal Response – [www.itu.int](http://www.itu.int)

<sup>18</sup> [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/246751/horr75-chap1.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf)

<sup>19</sup> [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/248621/horr75-chap2.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf)

<sup>20</sup> For the MIA statistical data see: <https://police.ge/en/useful-information/statistics>

<sup>21</sup> [https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime\\_what-is-it.html](https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html)

<sup>22</sup> Ibid.

<sup>23</sup> <https://www.cnbc.com/2019/09/21/saudi-aramco-attacks-could-predict-cyber-warfare-from-iran.html>

<sup>24</sup> <https://www.bbc.com/news/technology-40706093>

<sup>25</sup> <https://www.bbc.com/news/world-us-canada-55374945>

## 2. Main Cybercrime Threats

Regulatory framework for the cyber sphere and accordingly, the first legal understanding of cyber threats has been developed in Georgia since the adoption of the Law on Information Security in 2012.<sup>26</sup> The first National Cybersecurity Strategy (NCS) adopted in 2013 offered an early overview of national cybersecurity threats and expanded understanding of cybersecurity threat notion. Since then, the national cyber threat landscape has been widely described in all three NCSs of Georgia including the latest draft of the upcoming one.<sup>27</sup>

Particularly, the latest draft of the NCS identifies the main categories of cyber threats: cyber warfare, information warfare, cyber espionage, cyberattacks orchestrated by state-run actors, cybercrime (including attacks against critical infrastructures (CIs)). The draft of the strategy states that cybercrime including unauthorized access to computer systems, unlawful possession of computer data, data infringement, unauthorized use of computer equipment, crimes relating to child pornography and violation of intellectual property is widely prevalent. Especially significant forms of cybercrime can be found in the forms of the so-called phishing, identity theft, and use of malware and deface. The most prevalent attacks against CIs that have been seen in recent years are phishing, ransomware, deface, DDoS, email spoofing.

Cybercrime threats are also defined in the draft Strategy for Combating Organized Crime, which identifies transnational cybercrimes and state-sponsored organized crimes (e.g., cyberterrorism) as the emerging cyber threats. According to strategic threat analysis, numbers as well as the sophistication of cybercrime cases have been increased; most common threat actors tend to be both individual criminals, spies, malicious cyber actors, organized groups, terrorists and national state actors.

National and transnational criminal trends in cybercrime are periodically identified by the international, regional and leading national Law Enforcement Authorities (LEA) of developed countries having close cooperation with the MIA. The analysis made by international and foreign partners is important to understand Georgian cybercrime threats in a wider context. Namely, various analytical documents of Interpol,<sup>28</sup> Europol<sup>29</sup> and

---

<sup>26</sup> <https://matsne.gov.ge/en/document/view/1679424?publication=3>

<sup>27</sup> Final draft of National Cybersecurity Strategy and Action Plan 2021-2023 available as a paper copy to a researcher.

<sup>28</sup> See Interpol assessment of global cybersecurity landscape, available at: <https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats>

<sup>29</sup> See: IOCTA 2020 prepared by EUROPOL, available at: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020> and SOCTA 2017, available at: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017>.

FBI<sup>30</sup> have elaborated a well-established list of cybercrime threats mostly reflected in their strategic documents. It is noteworthy that the threats described in renewed Georgian national draft strategies echo those listed in various reports of Interpol, Europol and FBI. Based on the analysis of international and national strategic documents, these are the most common cybercrime threat vectors in Georgia:

**Darkweb** – Cybercrime as a Service (CaaS).<sup>31</sup> The dark web continues to enable a range of criminality that threatens the world, as well as Georgia. Despite the LEA's attempts to take down multiple sites, the dark web continues to hold a large number of sites hosting offensive images, as well as forums about OCSA. Large scale, multi-vendor markets remain the principal source of trading in criminal commodities on the dark web, with sites selling drugs, weapons, malware and false documentation. Criminals continue to use virtual assets, such as Bitcoin, to buy and sell commodities on illicit online marketplaces and to launder criminal profits.

### Georgian Darkweb Case:

*In November – December of 2019, MIA conducted operative – investigatory measures and revealed illicit drug trading through darknet (approximate illegal drug trading amounted to 6 mln GEL), closed 15 online drug distribution stores and drug laboratories in Tbilisi and Batumi. In total, 38 members of online drug dealers were arrested (including foreign citizens).*

 [https://www.radiotavisupleba.ge/a/30345527.html?fbclid=IwAR2iB4r\\_bpeu-F8qyUW1hsp4t0u41u35q40tWQB2j9Fc84H5boynV7HVpAaw](https://www.radiotavisupleba.ge/a/30345527.html?fbclid=IwAR2iB4r_bpeu-F8qyUW1hsp4t0u41u35q40tWQB2j9Fc84H5boynV7HVpAaw)

**Malware** - a composed term of different malicious cyber activities like spyware, trojans, ransomware, virus, and worm, etc.<sup>32</sup> Malwares in different forms and methods are evolving year after year to steal and manipulate data, disrupt computer programs and operation of critical information systems, hinder the functioning of infrastructures and access to it.

---

<sup>30</sup> <https://www.fbi.gov/investigate/cyber>

<sup>31</sup> <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020>

<sup>32</sup> “Malware is a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners” Organization for Economic Cooperation and Development (OECD) [https://www.oecd-ilibrary.org/science-and-technology/computer-viruses-and-other-malicious-software/an-overview-of-malware\\_9789264056510-3-en](https://www.oecd-ilibrary.org/science-and-technology/computer-viruses-and-other-malicious-software/an-overview-of-malware_9789264056510-3-en)

## Cyber Espionage – Advanced Persistent Threat actions (APT28):

*APT28 is a threat group attributed to Russia's General Staff Main Intelligence Directorate (GRU). Its common tactic is to send phishing emails with specific topics (lures) relevant to target victims. This increases the likelihood that recipients will believe that the email is legitimate and will be interested in opening the message and any attached files or clicking on a link in the body of the email. APT28 aimed to collect intelligence about Georgia's security and political developments toward NATO and EU integration by targeting officials working for the Ministry of Internal Affairs and the Ministry of Defense.*



<https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf>

**Ransomware** - The most reported way to directly extort funds from a victim is through ransomware attacks, where criminals encrypt data and then demand a ransom to decrypt it. The most targeted groups of ransomware attacks are both individuals and companies. Accounting systems and financial documents of SMEs are frequently under successful attacks. It appears that cyber hygiene rules such as creating reserve copies and having strong mail passwords are not well-followed that makes these target groups common cyber victims.

## WannaCry Ransomware:

*It is the most popular ransomware globally, effecting hundreds of countries, thousands of organizations in different sectors (healthcare, mobile telecommunication etc.) causing big havoc and billions of dollars of damage in the world. WannaCry is a type of malware that penetrates the computer system, the files on local disks and network storage are encrypted. Once the files are encrypted, the criminals demand a ransom payment in exchange for the recovery of affected files. The US and UK governments have said North Korea was responsible for WannaCry affecting hospitals, businesses and banks across the world. WannaCry targets have been reported in Georgia (e.g. commercial banks), but they prefer to stay anonymous.*



<https://www.facebook.com/certgovge/posts/506897886100466/>

The use of **Phishing emails** – emails containing malicious content – remains the most commonly observed method to deliver malware. The past year has seen a change in the content of phishing emails, with fewer malicious attachments and more links to malicious websites. Spam e-mails are often used for phishing purposes according to CERT.

GOV.GE<sup>33</sup>. E-mail-based phishing typically occurs in three phases: 1) Criminals identify legitimate companies that are offering online services and communicating electronically with customers; 2) They design websites that look like the legitimate websites of the identified company, known as “spoofing sites.” Users are redirected to “spoofing sites” that request the user to provide details such as passwords and other information that can be used for identity theft; 3) use the information disclosed by the victim to log on to the victim’s accounts and commit offences, such as transferring money or applying for new accounts.<sup>34</sup>

## Phishing

*Phishing was the most commonly used cybercrime targeting the financial and banking sector in Georgia in 2019-2020. Phishing is conducted by a fake web-page designed for stealing information, most commonly banking data for Georgians. . The address and content of the fake web-page resemble those of the original web-page, the user usually doesn’t pay attention to the URL and considers it to be the real web-site. In case of one of the commercial banks of Georgia, the domain tbcOnline.ge included zero instead of letter «O», thus misleading the user.*



<https://www.nbg.gov.ge/index.php?m=340&newsid=3644>

**Business Email Compromise (BEC)** is one of the fastest-growing threats, especially for small businesses. Criminals imitate an employee or a common supplier of a company – usually requesting payment of an invoice – by using compromised credentials to seem credible. More precisely, cybercriminal carefully investigates e-mail communication practices between business partners, vendors and suppliers. After illegally accessing the e-mail of a client, cybercriminals send the company forged invoices with falsified bank account information and wrong credentials. The target company believes the invoice and e-mail to have correct data and transmits money to the cybercriminal’s account.

*According to the FBI report, between October 2013 and May 2018, over 78,000 reported incidents accounted for over 12 million USD in losses in the USA. Targets of BEC in Georgia frequently are SMEs.*



<https://www.facebook.com/europeanunioningorgia/videos/795820687632137/>

<sup>33</sup> CERT. GOV. GE’s official FB page - <https://www.facebook.com/certgovge/posts/2098502846939954>

<sup>34</sup> <https://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf>

**Online Fraud** - Data remains the key commodity for cyber criminals, and there are several ways to exploit it for financial gain. Identify theft, data mining, personal data compromise – these are the most common cyberattacks targeting various types of confidential information often for criminal gain. Cybercrime is a major enabler of fraud: data obtained via data breaches, phishing and malware are used directly to commit fraud data is sold online to enable others to commit illegal activities. Another key enabler is social engineering, where fraudsters manipulate victims into handing over money or personal information, often informed by data they have researched, bought or hacked online. In previous years, SIM Box fraud was very popular in Georgia (re-shifting of international calls so that they appear to be the local once and causing material damage to victim companies and individuals), followed by PayBox Frauds (attacker perpetrating into the computer system and illegally transferring money).

### Online Shopping Fraud

*There are dozens of cases when Georgian citizens do online shopping with FB registered online shops that promise to deliver the goods in return for paid price. In many cases FB online shops are fake and a source of fraud. Users select goods, make an order, transmit money, but the online shop neither provides the bought commodity, not returns money back. Moreover, if an online shop gets access to credit card requisites of a buyer, as a buyer itself provides its personal banking data without a doubt, cybercriminal easily withdraws available money from the deceived buyer's account.*

*Widespread cyber banking fraud in Tbilisi and Kutaisi could be described like that: Cybercriminal, disguised as a bank officer, called/sent SMS to a bank client – target victim with a deceitful aim to settle a problem associated with his/her existing account or as an employer with a task to open a banking account. Potential victim, having no doubt in the identity of a caller, provided personal and banking card data, e.g. 16 digit number, duration of the card, CVC codes to a cybercriminal who afterwards withdrew money from a victim's account and even more, opened multiple credit products in different banks on behalf of the client.*



<https://www.youtube.com/watch?v=pfM8Ac1Nwel>

<https://www.youtube.com/watch?v=zolqcWTZT5I>

**Deface, DDoS** - Denial of service attacks trigger computer systems and infrastructure unavailable to users. The most common targets are government sites. There are multiple ways how DDoS attacks are conducted, e.g.: sending malformed queries to a computer system, exceeding the capacity limit for users, and sending more e-mails to e-mail serv-

ers than the system can receive and handle<sup>35</sup>. One of the recent cases of this year effected the University of Georgia whose site has been defaced and allegedly, personal data from university internal systems have been leaked.<sup>36</sup> If we compare DDoS attacks with the ones back from 2008, we can assess that attacks have been increased in scope and became more massive, while Internet Service providers (ISP's) do not have the required DDoS protection tools in order to tackle the attacks. The most DDoS targeted entities in Georgia are hosting providers.

### October 2019 – Massive Cyber Attack

*One of the massive cyber-attack on Georgian Cyberspace - around 15,000 websites in Georgia including those of major government institutions, broadcasters and online newspapers, and private businesses have been hit by a large-scale cyber-attack. Broadcasting companies TV Pirveli, Maestro, GDS were unable to broadcast for certain hours, their portals were blocked and access to servers denied. Georgian online news outlets Tabula and Georgia Today were inaccessible for the same period, dozens of websites belonging to state agencies, including the one of President of Georgia, the Appeals Court, the Adjara Government and other regional entities, watchdog groups like the Media Development Foundation, and the Free University were also affected by defacement. Most of the hacked websites were not operational with a demonstrated image of a former Georgian President Mikheil Saakashvili with the text: "I'll be back".*

*According to the State Security Service of Georgia (SSSG), the cyberattack aimed to undermine Georgia's national security, harming the Georgian population, disrupting the functioning of government agencies, as well as various organizations, and stirring commotion and sowing unrest in public. The Georgian Interior Ministry has launched an investigation into "unauthorized access to a computer system" and "Illegal use of computer data and/or computer systems". According to the investigation conducted by the Georgian side and the information received as a result of cooperation with international partners, the cyber-attack was planned and carried out by the Special Division of the General Staff of the Armed Forces of the Russian Federation.*

 <https://www.bbc.com/news/technology-50207192>

<sup>35</sup> <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e9c49>

<sup>36</sup> <https://formulanews.ge/News/32293>

## 2015 DDoS on Georgian Financial Sector:

*During the 4 days of May 2015, the Georgian Financial Sector, including the Financial Analytical Service of the Ministry of Finance, TBC Bank, Georgian Card and others have become victims of massive cyber-attacks promulgated by 339 000 unique IP addresses from more than 160 countries. When analyzing the attack and log-files of victim organizations, CERT.GOV.GE identified that hackers had launched “UDP Amplification” attack (an attack that relies on publicly accessible User Datagram Protocol and overwhelms a victim’s system with UDP traffic). Namely, with IP spoofing offender used the IP address of targets to send thousands of requests to the open UDP services that responded to the targets’ IP addresses. This made their service disrupted and un-operational.*



Information from CERT.GOV.GE

**Misinformation, Information Attacks, Fake News** – all these terms are shortly called as “Information Influence Operations”, which by modification or manipulation with data or introduction of contradictory data aim to influence a political or business outcome. It also concerns with destabilization of various social groups or the whole country. This threat becomes a more challenging visible element of hybrid war. Initially, this type of threat aimed to achieve political objectives and was mostly considered as a theoretical concern of national security communities, without directly and visibly touching law enforcement and criminal justice domains. However, the COVID-19 pandemic revealed the practical results of this threat and pushed it into the focus of Interpol as a cybercrime threat.<sup>37</sup>

---

<sup>37</sup> See Interpol report on cybercrime threats during COVID-19 pandemic, available at: <https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19;>

## Hacking, Falsifying, Misleading:

*On September 1, 2020, a cyberattack was carried out on the computer system of the Ministry of Internally Displaced Persons from the Occupied Territories, Labor, Health and Social Affairs of Georgia (“Ministry”). Based on the evidence, the cyberattack was carried out by foreign special services of the Russian Federation with the aim of unlawful possession, use of medical records and pandemic management information stored in the Ministry, as well as in the Richard Lugar Center for Public Health Research (Lugar Laboratory) in Tbilisi. Part of the authentic documentation obtained as a result of illegal intrusion was deliberately falsified and uploaded on one of the foreign websites aiming to cause intimidation, confusion and destruction of the public. It is not the first time when Lugar Laboratory has been targeted by Russian authorities in order to criticize its activities and accuse it in the spread of different illnesses allegedly supported by the US government.*



<http://georgiatoday.ge/news/22260/MIA%3A-Cyber-Attack-Carried-Out-on-the-System-of-Lugar-Lab>

### 3. Cybercrime Statistics

To understand how these threats are embodied into practical results and damage society, it is necessary to look at official statistics of registered cybercrimes. This data reflects how many of the above-listed threats have been realized in practice and gives primary information for measuring the state of affairs regarding cybercrimes. There are two main indicators: statistical data of the MIA and statistical data of the CERT. As it was mentioned above, the MIA considers only cyber-dependent crimes defined by Articles 284-286 and 3241 of the Criminal Code of Georgia (CCG) under cybercrime statistics. Information on cyber-enabled crimes is not included under cybercrime statistics and is not available publicly. Therefore, the Georgian public witnessed several major cyber-enabled criminal cases such as transnational child-pornography, when the Georgian Police in cooperation with foreign colleagues dismantled the international set of child pornography industry operating in Georgia.<sup>38</sup> This also makes an assessment of Georgia’s cybercrime reality very challenging. Independent Georgian experts believe that, the analysis of illegal activities envisaged by at least the following 12 Articles of CCG should be conducted to understand the real state of affairs in terms of cybercrimes in Georgia.<sup>39</sup>

---

<sup>38</sup> <https://police.ge/en/politsiam-arasrultslovnemis-pornografiis-ukanonod-damzadeba-gasaghebi-sa-da-trefkingis-braldebit-organizebuli-danashaulebrivi-qselis-kidev-11-tsevri-daakava/13160>

<sup>39</sup> Interview with Georgian Expert Giorgi Pirveli;

**Table 1.** Article of the CCG envisaging cybercrimes: including cyber-dependant and cyber-enabled crimes:

Article 151	Stalking
Article 157	Violation of privacy or personal data protection
Article 158.	Violation of the secrecy of private communication
Article 159.	Violation of secrecy of personal correspondence, phone conversations or other kinds of communication
Article 189	Violation of the rights of a holder of copyright or allied rights and the rights of database manufacturers
Article 210	Manufacturing, sale or use of forged credit cards
Article 255	Illegal production or sale of a pornographic work or other items
Article 284	Unauthorized access to computer system
Article 285	Illegal use of computer data and/or computer system
Article 286.	Unauthorized handling of computer data and/or computer systems
Article 314	Espionage
Article 324 <sup>1</sup>	Cyberterrorism

Before 2017, cybercrime was a trend that increased every year. Cybercrime cases registered by the Georgian Police remained under 500 cases in a year, which did not seem alarming in the light of the total 33 000 - 35 000 criminal cases registered annually by the police.<sup>40</sup> The first signs of significant changes in this domain emerged already in 2018. The trend of permanently raising cybercrime statistics remained unchanged but the speed of the rise was dramatically changed.

**Table 2.** Registered cybercrimes in Georgia 2017 - 2020:<sup>41</sup>

Year	Number of Registered Cyber-crimes	% Rate +/- In Comparison with Previous Year	Number of Resolved Cyber-crimes	% Rate of Resolution	Total Number of Registered Crimes	% Rate of Total Registered Cyber-crimes
2017	506	-8%	254	25.3%	37 944	1.33%
2018	1268	+150.59%	98	7.73%	58 412	2.17%
2019	1806	+42.43%	98	5.43 %	64 123	2.8%
2020	2143	+18.66%	206	9.61%	56 596	3.78%

<sup>40</sup> <https://info.police.ge/cat?id=88>

<sup>41</sup> Source: statistical data provided by the MIA, available at: <https://info.police.ge/page?id=115>

152 cybercriminals were detected by the Georgian Police in 2020.<sup>42</sup> According to the threat analysis and cybercrime statistics from the Cybercrime Unit of the CCPD, the numbers of cybercrimes as well as the sophistication of the cases have been increased, but the investigation rate has drastically decreased.

The analysis of cybercrime statistics in a broad context of criminal situation in Georgia makes obvious that pure cybercrime still does not pose a serious danger for general public safety environment. Firstly, despite increasing figures, the share of cybercrime within general criminal statistics is still relatively small. In a four-year perspective, cybercrime never exceeded 4% of total criminal cases registered by the police. A total number of criminal cases also increased in these four years, but the share of pure cybercrime in this trend was not significant. Secondly, there are no signs that cybercrime is replacing other types of illegal activities in Georgia. Contrary, a very alarming trend observed in some developing countries.<sup>43</sup> Finally, there are no publicly available reports or news about significant financial losses or other economic damages resulted from cybercrime in Georgia.

However, another important issue regarding the official cybercrime figures is how fully they reflect the real situation on the ground. High latency of certain types of crime is not uncommon problem for the Georgian Police and the experience of domestic violence crimes witness this.<sup>44</sup> When it comes to cybercrime, it is widely recognised that even in developed countries with great policing traditions, LEAs face the problem of underreporting.<sup>45</sup> This is trending in Georgia's close neighbourhood as well, where public awareness and trust towards police is low. As Cybercrime is a relatively new phenomenon in Georgian society, there is a high probability that many cybercrimes are underreported, especially taking into account the low level of public awareness.<sup>46</sup> If we look at the figures of reported cybercrime by regional police departments, it is evident that in Tbilisi, where general public awareness is higher, cybercrime reporting is relatively high than in other regions. For example, in 2019, 1084 cases were reported in Tbilisi, with 1

---

<sup>42</sup> <https://www.interpressnews.ge/ka/article/634016-2020-cels-policiis-mier-dakavebuli-da-pasux-isgebashi-micemulia-152-kiberdamnashave>

<sup>43</sup> Official data provided by the MIA Georgia indicates that property crimes (articles 177-189 of Georgia's criminal code), which are usually substituted by cybercrimes, remained generally on the same level or even tended slightly to increasing in 2017-2020. Detailed information is available at: <https://info.police.ge/page?id=115>

<sup>44</sup> Domestic violence was mainly underreported in Georgia until 2017 and after the MIA implemented impressive awareness raising campaign registered domestic violence cases almost doubled in 2018. See: <https://info.police.ge/uploads/5c595f186e358.pdf>

<sup>45</sup> [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/246751/horr75-chap1.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf)

<sup>46</sup> The Georgian Police have already experienced similar situation regarding domestic violence, which was one of the most underreported type of crime in recent years. The police have undertaken very active and serious work, including awareness rising campaigns to improve reporting and then properly handle this type of crimes.

184 800 population, more than 60% of all registered cybercrimes nationwide, while in Imereti region with 487 000 population only 126 cases and in Kvemo Kartli region with 434 200 population only 68 cases were reported.

Georgian expert community believes that although there is a noticeable increase in the number of cybercrime year after year, still cyber criminality is underreported due to a lack of trust in the capacity of the cybercrime investigation.<sup>47</sup> This makes it difficult to provide a comprehensive analysis of a realistic picture of the Georgian cybercrime state of play, as well as estimate the scale and cost of it to the state, its economy and people. So, in this context it is important to look at another indicator – statistics of registered incidents to summarize quantitative assessment.

#### **4. Cyber Incidents Statistics**

The key source for collection and analysis of cyber-related incidents in any country are CERT communities. In Georgia, CERT.GOV.GE of DGA is a national and government cybersecurity authority that ensures the safety and resilience of cyberspace; it also supports public and private entities to deal with threats and incidents in this domain.<sup>48</sup> From the perspective of this research, the most important function of the CERT is to launch different tools and technics for detecting and handling incidents in cybersphere. It represents an essential source for LEA`s information about cyber threats and possible cybercrime cases.

Statistical data collected by the CERT through the use of various technological means (network and IP monitoring system, portals, sensors etc.) makes it clear that the number of registered incidents within the period from 2014 to 2019 at least doubled. The number of infected IP addresses was also elevated, including cyber events relating to various portals. During a performance of its duties, CERT utilizes different incident management platforms for incident collection, detection and processing, these are: (a) Cyber Incident Management System, (b) Checknet, (c) IP address Monitoring Portal, (d) Network Monitoring Portal.<sup>49</sup> These platforms are briefly described below.

- a) Cyber Incident Management System Platform allows CIs to share the information on cyber incidents with CERT.GOV.GE in a fast and efficient way and to monitor the incident handling process. This system promotes the centralization of the cyber-incidents and the creation of a single cyber incident database.

---

<sup>47</sup> Interview with Georgian cybersecurity expert Irakli Lomidze.

<sup>48</sup> <https://matsne.gov.ge/en/document/view/1679424?publication=3>

<sup>49</sup> Information regarding incident reporting tools, technics and statistical data reflected in this sub-chapter is provided to a researcher by CERT.GOV.GE.

**Table 3.** Cyber incidents collected through Cyber Incident Management System (2014-2020)

<b>Year:</b>	<b>Cyber Incidents</b>
2020	660
2019	536
2018	812
2017	795
2016	1264
2015	486
2014	291

CERT.GOV.GE makes incident classification in accordance with the European Union Agency for Network and Information Security (ENISA) "Reference Incident Classification Taxonomy".

**Table 4.** Classifications of cyber incidents according to ENISA

<b>Cyber Incident</b>	<b>2017</b>	<b>2018</b>	<b>2019</b>	<b>2020</b>
<b>Abusive Content (spam)</b>	2	9	16	5
<b>Availability (DoS, DDoS)</b>	8	2	3	13
<b>Fraud (phishing)</b>	14	12	408	300
<b>Intrusion Attempts</b>	640	745	39	13
<b>Malicious Code (virus, worm)</b>	36	34	42	102
<b>Other</b>	62	3	2	1
<b>Vulnerable (open for abuse)</b>	33	7	26	226

- b) Checknet is another proactive security service of CERT.GOV.GE which is widely and freely available to any party interested to get information whether their web sites and IP addresses are cyber vulnerable or have been hacked. In case of a security breach, the system advises the customer about the type of cyber vulnerability – defacement, malware, phishing, etc. There are 8085 registered GEO web domains in total (e.g., ended with gov.ge) and they are uploaded on Checknet portal. Cyber incident analysed from Checknet system reveals that malware is the dominant cyber threat in the Georgian cyberspace with 67% of occurrence, while defacement comes second with 28.5% and phishing amounts to only in 4.4% cases. Due to a lack of resources, Checknet portal currently is not operational.
- c) IP Address Monitoring Portal – daily several dozens of infected IP Address located in Georgian cyberspace are uploaded in the portal. CERT/CSIRT gets these data from different international partners. Up to 40 government and private agencies are the consumers of the system and in the last 4 years, the portal collected data of 677 298 978 infected IP addresses out of which there are 243 151 unique IPs. If we look on a

daily statistic, CERT.GOV.GE receives 1000 to 10 000 security feeds indicating different types of security events with different levels of severity. These cyber events can indicate infection of computer systems, the existence of different malwares, human errors, DNC misconfigurations, etc. Due to a lack of resources, IP monitoring portal is not operational since 2018.

**Table 5.** Incidents reported to IP Monitoring Portal

<b>Year:</b>	<b>Incidents</b>
2018	177
2017	391
2016	356
2015	312
2012-2014	949

- d) Network Monitoring System –automatically analyses network flow security problems/anomalies and detects security breaches like DDoS attacks, botnets, etc. Network monitoring sensors are configured in less than 10 Cis and up to 2000 network anomalies were detected in the course of 4 years. Unfortunately, the network monitoring system has stopped its operation since 2017.

Analysis of cybercrime statistical data of the MIA and cyber incident data of CERT.GOV.GE reveals a high likelihood of a lack of uniformed standards, regulatory frameworks and common approach of cyber incidents and cybercrime registration, crime reporting and incident information sharing between authorities.

## 5. Main Threat Actors

Analysis of the cybercrime and cyber incident statistics, open-source data, analytical and policy reports lead to the conclusion that most cybercrime threats are originated from the following categories of threat actors:

- 1. Internal** –crimes are originated in Georgia as a result of criminal activities of individual criminals or small criminal groups (not belonging to organized crime in the traditional sense). These crimes are mostly related to unauthorized access of computer systems (breach of personal data, e-banking, e-gambling and etc.), ransomware and forged credit cards;
- 2. External** - crimes are originated in other countries as a result of attacks of state agencies or state-sponsored groups as an element of subversion or other hostile policy. The incidents caused by external attacks need to be registered as criminal cases for proper response through criminal justice procedures. These crimes are related to unauthorized access to computer systems and stalking;

**3. Transnational** – crimes are originated in Georgia or other country as a result of criminal activities of transnational organised groups when Georgia is part of the big transnational criminal transaction, (for example online child sexual abuse (OCSA), money laundering, Darkweb related operations and etc.) or criminal activities are organized/conducted by Georgian citizens and GOCGs operating abroad.

Currently, the MIA's most cybercrime cases are originated from internal and external threat actors. Increased access to the internet for Georgian citizens and businesses in recent years<sup>50</sup> without significant measures of awareness-raising and development of cyber hygiene among citizens created fertile soil for illegal activities and additional opportunities for emerging internal criminal actors. That is a well-known trend for European and CIS countries' LEAs, where internet access prompted the substitution of property crimes to cybercrimes.<sup>51</sup> That can serve as one of the explanations for raising of cybercrime rates in Georgia as well. In terms of the external actors of cybercrime, it is obvious that the Russian Federation utilizes multiple elements of hybrid warfare against Georgia<sup>52</sup> causing damage to thousands of Georgian entities and individuals.<sup>53</sup> Opening criminal investigation is a single legal remedy at disposal of the Georgian government agencies to seek international law enforcement organizations' assistance and political support for proper response.

The share of illegal activities of transnational organized groups in overall cybercrime statistics is not significant. The Georgian Police have reported few cybercrime cases<sup>54</sup> involving transnational organised crime. However, it has to be taken into account that handling of some transnational cybercrime cases is conducted by the Georgian Police without opening official criminal investigations.<sup>55</sup> This work is done through various international law enforcement cooperation frameworks under the special legislation.<sup>56</sup> Therefore, various assessments of international law enforcement organisations also wit-

---

<sup>50</sup> According to ITU, 68.85% of individuals in Georgia had access to the Internet in 2019, same indicator in 2010 - 26,90% and in 2000 0 0.48%. ITU data also shows that 75.8% of households in Georgia have Internet access at home. Georgian National Communications Commission (GNCC)'s data of 2019 state that number of mobile internet users in comparison with country population amounts to 93%, that is around 3,2 million people. GNCC 2019 report <https://www.comcom.ge/uploads/other/5/5671.pdf> and ITU World Telecommunication/ICT Indicators Database online (2020): <http://handle.itu.int/11.1002/pub/81550f97-en> (indicator "i99H")

<sup>51</sup> [https://www.ng.ru/economics/2020-09-10/1\\_7961\\_cybercrime.html](https://www.ng.ru/economics/2020-09-10/1_7961_cybercrime.html)

<sup>52</sup> See "Hybrid Threats in EaP Countries, Building Common Response" edited by Kakha Gogolashvili, pp.20-24; Available at: <https://www.gfsis.org/files/library/pdf/English-2739.pdf>

<sup>53</sup> <https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/>

<sup>54</sup> For example, OCSA case in 2019, Transnational crime – QAAZZ multi-million money laundering case in 2020 and etc., more information is available at: <https://police.ge/en/press-center/news>

<sup>55</sup> Relevant information about this type of work was provided by the MIA as a part of requested official information.

<sup>56</sup> The law of Georgia on international cooperation in LE sphere, available in Georgian at: <https://matsne.gov.ge/document/view/2048477?publication=5>

ness that transnational crime still has low connection with Georgian cyberspace. GOCGs are actively engaged in transnational criminal activities in the US, the EU and the CIS region, but open-source analysis indicates that they are mostly involved in conventional crimes with physical dimensions and low connection with cybersphere yet.

However, if we look at the wider picture, Russian speaking organized crime groups (GO-CGs are part of those), tend to explore cybersphere. Most serious cybercrime against the UK are perpetrated by Russian speaking organized crime groups<sup>57</sup>. Since the EU association process, the Georgian Police have been working against illegal activities of GO-CGs abroad very actively in the context of international law enforcement cooperation. Transnational organised crime as a source of the threat of cybercrime is acknowledged in many policy documents prepared by the MIA.<sup>58</sup> Notably, cybercrime is generally considered a threat in combination with organized crime. This source of threat is maybe not challenging in a short-term perspective, but it would be definitely on the rise in the long run. GOCGs engagement in illegal cyber activities seems to be a matter of time and is easy to predict considering European and CIS region trends.

---

<sup>57</sup> See the UK national cybersecurity strategy, available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/567242/national\\_cyber\\_security\\_strategy\\_2016.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf)

<sup>58</sup> <https://www.matsne.gov.ge/ka/document/view/3660371?publication=0>

## CHAPTER III. CYBERCRIME AND THE NATIONAL SECURITY

In many western countries' cybersecurity is an essential element of national security as a part of complex homeland security discourse (USA) or directly of the national security policy (Israel). In some countries, serious and organized crime (whether it is cyber-related or not) is unquestionably considered as an issue of national security (UK). In the post-soviet countries, cybercrime is generally considered as a part of criminal justice or policing (Armenia). In Georgia, there is still an ongoing process of shaping various angles of the national security policy.<sup>59</sup> Cybersecurity is already established as a solid element of the national security domain<sup>60</sup> and public order (public security in other terms) is also acknowledged as an area of the interest of the national security policy.<sup>61</sup> However, as publicly available official documents reveal and official public statements and speeches evidence, despite legal notions, in practice Georgian officials and field experts associate cybercrime with more criminal justice domain rather than national security or security policy issues.

The importance of cybersecurity for the national security context of Georgia is mainly determined due to the very nature of cybersphere. Security policy experts observe a significant raise of cybercrime as a powerful weapon for subversion by political means.<sup>62</sup> It is impossible now to secure the state and citizens only through protecting borders and undertaking sophisticated counter-intelligence measures as it was used to during the cold war. Cybersphere is vastly used by external threat actors to infiltrate deeply into any other country of interest and generate serious, sometimes even existential problems inside of that country, without application of any open conventional means and internationally disclosed hostile actions in peacetime. Massive cyberattack on Estonian banks, media and other important services in 2007 incurring losses of thousands of Estonian citizens was the first and exemplary case revealing how post-World War II legal and security systems were inadequate to the challenges emerging from new technologies.<sup>63</sup> When it comes to wartime, the cybersphere becomes the 4th dimension of warfare in the XXI century.<sup>64</sup>

With ICT's wide opportunities, there are two decisive factors, making cybercrime more complex and far-reaching than an issue of criminal justice or public safety. These two

---

<sup>59</sup> The legislation regulating formation of the national security policy was updated several times, the last was in 2019. Available at: <https://matsne.gov.ge/document/view/2764463?publication=10>

<sup>60</sup> Ibid.

<sup>61</sup> Ibid.

<sup>62</sup> Cath Senker, *Cybercrime and the Darknet*, Sirius Publishing, London, 2017, pp. 64-91.

<sup>63</sup> P.W Singer and Allan Friedman, *Cybersecurity and Cyberwar, What Everyone Needs to Know*, Oxford University Press, New York, 2014; pp 122-123.

<sup>64</sup> *Anatomy of Hybrid Wars*, edited by Tinatin Khidasheli, Tbilisi, 2020; pp. 91-105.

factors exist constantly since gaining Georgia's independence as important challenges to its national security. Certain external threats realized in various conventional (2008 Russia-Georgia war) and nonconventional or sub-conventional forms (misinformation campaigns aiming to erode social consensus on important issues, cyberattacks, etc.) and "thieves in law" organized crime tradition inherited from the Soviet Union already as a transnational phenomenon, expose serious danger to Georgia's National Security. These two in combination have significantly shaken Georgian statehood after the dissolution of the Soviet Union.<sup>65</sup>

The existence of strong external threat actors as sources of cybercrime in Georgia is one of the main reasons why the Georgian government needs to handle cybercrime issues more carefully than other types of crimes. It is widely perceived that the Russian Federation, with its gruesome reputation as one of the strongest and dangerous troublemakers in cyberspace globally,<sup>66</sup> permanently undertakes a wide array of overt and covert measures for subversion of its neighbours and not only.<sup>67</sup> 2019 and 2020 cyberattacks emphasize that Georgia is a target of various Advanced Persistent Threat (APT) campaigns conducted by Russian intelligence agencies and not only.<sup>68</sup> Russian subversion efforts were gradually refined and eventually shaped into the concept of Hybrid War.<sup>69</sup> This new type of warfare actively utilizes information technologies in many dimensions to achieve multiple goals. Especially, 2020 cyberattacks on the digital infrastructure of the Center for Public Health Research- an important part of Georgia's National Centre for Disease Control, popularly known as the Lugar Laboratory<sup>70</sup> was preceded by a long-term misinformation campaign to undermine its credibility.<sup>71</sup> This serves as a good example of the complexity of external threats Georgia's National Security is currently facing.

---

<sup>65</sup> For more detailed information about role of Organised Criminal in Georgian Society after dissolution of Soviet Union see materials of Research Conferences on Organised Crime at the Bundeskriminalamt in Germany (Transnational Organized Crime), available at: [https://www.bka.de/DE/AktuelleInformationen/Publikationen/Publikationsreihen/publikationsreihen\\_node.html](https://www.bka.de/DE/AktuelleInformationen/Publikationen/Publikationsreihen/publikationsreihen_node.html)

<sup>66</sup> Numerous cyber-attacks are attributed to Russian Federation state agencies and their proxies worldwide. Including the US government agencies, Germany, the UK Ukraine, Georgia, Organisation for the Prohibition of Chemical Weapons (OPCW) and etc. For detailed information see: The Past, Present, and Future of Russia's Cyber Strategy and Forces, prepared by RAND corporation, available at: [https://www.rand.org/pubs/external\\_publications/EP68319.html](https://www.rand.org/pubs/external_publications/EP68319.html)

<sup>67</sup> See RAND overview of Russian subversion against other countries including Georgia. Available at: <https://www.rand.org/pubs/perspectives/PE331.html>

<sup>68</sup> Interview with Georgian cybersecurity expert Giorgi Iashvili.

<sup>69</sup> See analytical report on hybrid threats to Ukraine's public security, available at: [https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok\\_XXI-engl-last.pdf](https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-engl-last.pdf)

<sup>70</sup> For example, see: <https://www.government.nl/documents/diplomatic-statements/2020/02/20/the-netherlands-considers-russia%E2%80%99s-gru-responsible-for-cyber-attacks-against-georgia>

<sup>71</sup> <https://factcheck.ge/en/story/37919-lugar-laboratory-in-georgia-russia-s-traditional-rigmarole>

Information warfare campaigns as an effort of influence-wielding through digital means run enormous risks for Georgia's developing society.<sup>72</sup> This type of threat becomes more and more sophisticated and difficult to handle for many countries worldwide. It reached such level that is especially acknowledged as a serious threat in many high-profile policy documents of various countries with developed security infrastructure. For example, this problem is well examined by Israeli experts. Israeli national security strategy characterizes this type of threat as sub-conventional and puts it alongside other types of cybersecurity problematics as very dangerous in the context of national security.<sup>73</sup> The threat of erosion of social cohesion and solidarity is considered in the State of Israel as an important challenge to the country's internal security.<sup>74</sup> Information warfare is envisaged as one of the instruments for the erosion of social solidarity. In Georgia, great information flows from diverse internal and external sources are observed, covering a wide range of political, social, cultural, economic issues. As a result, Georgian society becomes more and more fragmented in recent years, but no visible consistent policy is evident as a response.<sup>75</sup> Discussion in international scholarship and publicly available reports of various national LEAs and security agencies, international organizations and think-thanks indicate that misinformation becomes more and more problematic, governments seek remedy to enhance the resilience of their countries and societies in this field. Putting misinformation in the list of cybercrime threats by Interpol in its latest report on cybersphere<sup>76</sup> witness LEA's efforts worldwide to constrain this challenge by the legal framework of cybercrime. The government of Georgia is seeking ways to tackle this emerging problem as well and it needs to be more careful in this regard.<sup>77</sup>

In the modern world, a well-established and internationally recognised set of rules for dealing with hybrid warfare (including cyberwar) elements has not been developed yet.<sup>78</sup> The national criminal legislation still remains the single legal remedy (crimes against state, terrorism, cybercrimes and etc.) for formal response.<sup>79</sup> In this context legal understanding of cybercrime gains broader essence than reflection criminal activity registered by the police. As it can be figured out from open-source analysis and little

---

<sup>72</sup> See Analysis of Russian Disinformation Campaigns in Georgia, available at: [https://www.pmcg-i.com/publications\\_file/10f55f0475e3322c4.pdf](https://www.pmcg-i.com/publications_file/10f55f0475e3322c4.pdf)

<sup>73</sup> See analysis of Israeli national security strategy, available at: <https://www.washingtoninstitute.org/policy-analysis/guidelines-israels-national-security-strategy>

<sup>74</sup> Ibid.

<sup>75</sup> See Analysis of Russian Disinformation Campaigns in Georgia, available at: [https://www.pmcg-i.com/publications\\_file/10f55f0475e3322c4.pdf](https://www.pmcg-i.com/publications_file/10f55f0475e3322c4.pdf)

<sup>76</sup> See Interpol assessment of global cybersecurity landscape, available at: <https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats>

<sup>77</sup> See Analysis of Russian Disinformation Campaigns in Georgia, available at: [https://www.pmcg-i.com/publications\\_file/10f55f0475e3322c4.pdf](https://www.pmcg-i.com/publications_file/10f55f0475e3322c4.pdf)

<sup>78</sup> Anatomy of Hybrid Wars, edited by Tinatin Khidasheli, Tbilisi, 2020; pp. 142-147;

<sup>79</sup> Ibid.

pieces of information shared by the government institutions for this study, the dramatic jump in cybercrime in 2019 was mainly the result of massive Russian cyberattacks. Georgian experts believe that Russian hackers use Georgia's cyberspace as a testing ground for sophistication their modus operandi.<sup>80</sup> The same situation is observed in Ukraine,<sup>81</sup> being also one of the most targeted neighbours of Russia alongside Georgia. The developments in the geopolitical context around Georgia and the main trends in global cybersecurity leads to the assumption that the external threat actors will continue playing an active role in the formation of Georgian cybercrime figures in the next years.

As it was outlined above, GOCGs represent another important factor affecting the increase of cybercrime rates in a long-term perspective. Despite the fact that the influence GOCGs and operational space for their members currently are very limited in the country and they generally operate outside of Georgia, mostly in Europe and in CIS countries, GOCGs still remain significant threat actors for Georgia's internal security because of several reasons. The first is the nature of the criminal subculture with roots in Georgian society,<sup>82</sup> flexibility for adaptation to the new circumstances and ability to easily recruit new members from developing communities, vulnerable social groups with limited access to education and economic opportunities. The second one is its transnational character. GOCGs as organized criminals from other post-soviet (currently CIS region) countries are strongly tied or even deeply integrated into the Russian speaking organized crime groups' subculture. Many of them operate as a part of Russian-Organized Crime Gangs within the Russian Federation and abroad. The criminal subculture exposes serious risk for any society, but in Russia's neighbourhood, it gains additional discourse. Case of the Baltic States witnesses that Organised Criminal Groups are effective instruments of subversion at disposal of Russian intelligence agencies.<sup>83</sup> Cases of utilisation criminal actors inside the country for undermining public security by external adversaries as a mean of hybrid war are observed in Ukraine as well.<sup>84</sup> In Georgia, this opportunity is limited due to strict legislation and the coherent approach of the Georgian Police. Not even small serious organized criminal groups are detected in the country and Georgian Police still manage successfully keeping down GOCGs out of the country, but cyber space exposes serious challenge in this regard as it affords the possibility of avoiding state borders and checkpoints. The first signs of the utilization of information technologies by GOCGs to

---

<sup>80</sup> Interview with Georgian cybersecurity expert Giorgi Iashvili.

<sup>81</sup> See analytical report on hybrid threats to Ukraine's public security, available at: [https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok\\_XXI-engl-last.pdf](https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-engl-last.pdf)

<sup>82</sup> Georgia's Public Defender admitted existence of certain problems of influence of the criminal subculture in the penitentiary system of Georgia in her recent report. Available at: <https://www.ombudsman.ge/res/docs/2020033122424787329.pdf>

<sup>83</sup> See RAND analysis "Hybrid Warfare in The Baltics". Available at: [https://www.rand.org/pubs/research\\_reports/RR1577.html](https://www.rand.org/pubs/research_reports/RR1577.html)

<sup>84</sup> See analytical report on hybrid threats to Ukraine's public security, available at: [https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok\\_XXI-engl-last.pdf](https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-engl-last.pdf)

infiltrate and perpetrate cyber-enabled crime are already visible.<sup>85</sup> Apart from that, the first major transnational (cyber-dependant) criminal cases are also reported with the active participation of Georgian criminals.<sup>86</sup> It is also noteworthy that GOCGs presence in the EU countries was actively boosted by Russian backed media resources in Europe as a hindrance and a cause for stalling of the process of Georgia's visa liberalisation. This is an interesting aspect of information warfare against Georgia which is not fully explored yet. During the EU visa liberalisation process, certain cases of misinformation campaigns were detected in Germany with the dissemination of speculative information about Georgian emigrants allegedly committing serious criminal offences, similarly to the case of fake news with a Russian girl allegedly raped by emigrants from Eastern Europe in Germany, to form a negative social opinion and make pressure on German politicians.<sup>87</sup> Unfortunately, in-depth analysis of this aspect goes beyond of the scope of the study.

Even countries with a highly developed internal security infrastructure, long-standing policing traditions and more mature self-organized societies, pay much more attention to serious and organised crime in the context of national security. The UK National Security Strategy and Strategic Defence and Security Review are exemplary in this regard for the GOG, still traditionally considering criminality as a part of criminal justice policy.<sup>88</sup>

In light of these developments, cybercrime is still an emerging phenomenon with unexplored potential in Georgian social life. It stands at the very edge between public safety, criminal justice and the internal security domain of the national security policy. Due to its unlimited capabilities, cybercrime threats and their affecting factors expose more systemic danger for Georgian society than armed robberies, or other property crimes and even domestic violence, which is observed as a problem of utmost importance for the Georgian Police in recent years. Cybercrime represents the crime of tomorrow<sup>89</sup> and the Georgian LEAs and security sector need to be more prepared to effectively handle it. It means more investment, more knowledge accumulation and mature approach.

---

<sup>85</sup> See virtual "Razborka" example: <https://police.ge/ge/shss-m-qurduli-samkaros-tsevrobis-braldebit-2-piridaakava/10342?print=1>

<sup>86</sup> <https://agenda.ge/en/news/2019/1299>

<sup>87</sup> Anatomy of Hybrid Wars, edited by Tinatin Khidasheli, Tbilisi, 2020; pp. 310-320;

<sup>88</sup> See the UK National Security Strategy, available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/555607/2015\\_Strategic\\_Defence\\_and\\_Security\\_Review.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/555607/2015_Strategic_Defence_and_Security_Review.pdf)

<sup>89</sup> P.W Singer and Allan Friedman, Cybersecurity and Cyberwar, What Everyone Needs to Know, Oxford University Press, New York, 2014; p. 85.

## CHAPTER IV. TRENDS IN THE NEIGHBORHOOD

Georgia is still at an early stage of formation of criminal justice and security policy in this domain, where there is still some uncertainty more prevailing. In this regard and for better understanding Georgia's situation regarding cybercrime, it would be helpful to look at some countries, with similar cultural context, political and economic developments and security problematic, also transnational criminal interconnections. Azerbaijan, Armenia, Ukraine and the Russian Federation were selected on the bases of these criteria. In addition, the European context in general, as well as EU Member States' – Lithuanian example, are also analysed as a more mature model for comparative considerations.

### 1. Azerbaijan

Public order in cyberspace of Azerbaijan is administered by the Ministry of Transport, Communications and High Technologies and the Ministry of Internal Affairs. The Ministry of Internal Affairs of Azerbaijan follows the same institutional model as Georgian MIA, vesting the authority on its Main Division for Combatting Organised Crime (analogue to Georgian CCPD) to handle cybercrime on centralized manner.<sup>90</sup> In all other issues, Azerbaijani experience significantly differs from the Georgian one. On the official level, Azerbaijani LEA never discusses problems regarding cybercrime publicly and in official crime statistics published either by the Ministry of Internal Affairs or General Prosecutor's Office usually, there are no figures about cybercrime rates.<sup>91</sup> Even the analysis of criminal situation conducted under semi-official scholarship, there is no overview of cybercrime-related issues.<sup>92</sup> Although there are several reports about certain cybercrimes in Azerbaijan,<sup>93</sup> it is widely perceived that cybercrime is not a common problem there.<sup>94</sup> This silence of Azerbaijani LEA might indicate that the authorities consider illegal activities in cybersphere mostly in the wider context of the internal security policy<sup>95</sup> than as an issue of criminal justice. Various reports on international attacks on the Azerbaijani cybersphere makes this implication stron-

---

<sup>90</sup> <https://mia.gov.az/?/en/content/272/>

<sup>91</sup> <https://az.sputniknews.ru/infographics/20191031/422184022/Prestupnost-v-Azerbaydzhane-tsfyry-i-fakty.html>

<sup>92</sup> See for example article of Nazim Aliyev, the head of the Academy of the Ministry of Internal Affairs of Azerbaijan: "Состояние, структура, динамика, и уровень преступности в Азербайджане", ЖУРНАЛ ЗАКОН И ПРАВО, №4.2020. pp. 28-40; available at: <https://www.elibrary.ru/item.asp?id=42694479>

<sup>93</sup> See examples at: <https://www.rferl.org/a/azerbaijan-hackers-banks/28637057.html> and

<https://news.az/news/azerbaijan-detains-two-bulgarian-nationals-over-cybercrime-in-banking-sector>

<sup>94</sup> <https://www.osac.gov/Country/Azerbaijan/Content/Detail/Report/6c4c0264-f96b-4474-8221-189e2a26a68e>

<sup>95</sup> The term of homeland security is used in the US to describe this domain of security.

ger.<sup>96</sup> Azerbaijani cyber ecosystem has similar sources of threats as Georgia: internal, external, transnational organized criminal groups. Due to the absence of publicly available reliable information, it's difficult to assess the share of these threat actors in the generation of cybercrime statistics.

## 2. Armenia

In Armenia cybercrime statistical data is not provided separately in publicly available general criminal statistics. As it can be figured out from open sources, cybercrime rate is increasing every year in 20-25% diapason in Armenia in recent years.<sup>97</sup> But it is highly likely to still stay below of 5% threshold of around 25000-26000 totally registered criminal cases annually.<sup>98</sup> According to assessments of the local experts, cybercrime remains mainly underreported in Armenia due to low public awareness.<sup>99</sup> Currently, cybercrime does not expose a significant problem in Armenia in the sense of the criminal situation.<sup>100</sup> The main threats are originated from internal and external sources.<sup>101</sup> No big cybercrime case was reported with the involvement of transnational organised criminal groups either by Armenian police or foreign and international LEAs.

## 3. Russian Federation

Cybercrime becomes more and more topical issue in the Russian LEA's agenda as there is observed impressive raise in cybercrime rates. The Ministry of Internal Affairs of the Russian Federation (MIARF) has been treating it as a growing specific problem since 2017. Illegal activities committed using means of information technologies (as cyber-dependant as cyber-enabled crimes) were not identified and calculated as a separate category of crime in MIARF's official criminal statistics bulletins before 2017.<sup>102</sup>

---

<sup>96</sup> See more information at: <https://www.securityweek.com/hackers-targeting-azerbaijan-show-interest-scada-systems> and <https://en.armradio.am/2020/10/11/azerbaijani-banking-system-hacked/> and <https://www.turan.az/ext/news/2020/7/free/Social/en/125740.htm> and <https://armenpress.am/eng/news/691881/ar>

<sup>97</sup> <https://armenpress.am/eng/news/937066/>

<sup>98</sup> <http://www.ksgp-cis.ru/about/obzory/sostojanie-prestupnosti-v-2019-godu>

<sup>99</sup> <https://newsarmenia.am/news/society/ekspert-nazval-samye-rasprostranennye-v-armenii-ugolovnye-kiberprestupleniya/>

<sup>100</sup> <https://www.osac.gov/Country/Armenia/Content/Detail/Report/ec92ebb9-be6a-4328-9e50-18a2c0147aca>

<sup>101</sup> For more information regarding Armenia's external threats, see: <https://www.refworld.org/docid/4ac62c3228.html> and <https://report.ge/en/world/azerbaijani-hackers-attacked-armenian-websites/>

<sup>102</sup> More information is available at official resource of the Ministry of Internal Affairs of the Russian Federation: <https://xn--b1aew.xn--p1ai/reports/item/9338947/>

**Table 7.** Cybercrimes registered in Russian Federation<sup>103</sup>

Year	Number of Registered Cyber-crime Cases <sup>104</sup>	Total Number of Registered Criminal Cases	Rate +/- In Comparison With Previous Year
2017	90 587	2 058 476	-----
2018	174 674	1 991 532	92.8%
2019	294 409	2 024 337	68.5%
2020	510 396	2 044 221	73.4%

Figures published by the MIARF demonstrates that cybercrime (including both - cyber-dependant and cyber-enabled cybercrimes) rates increased while the general criminal statistics threshold remains on the same level with minimal variability. It has to be underlined that the rise of cybercrime in the Russian Federation takes place simultaneously with the reduction of other traditional property crimes such as hijacking and theft, etc.<sup>105</sup> There is an emerging trend that illegal activities in the virtual sphere have been replacing criminal acts in physical space. Despite periodical claims of Russian authorities on cyberattacks organized from abroad,<sup>106</sup> it can be implied from the official Russian policing guidelines that, the main reasons for such significant raising cybercrimes are related to internal criminal threat actors.<sup>107</sup> Boost of digitalisation and expanding availability for access to information technologies for the wider population are considered as one of the important factors affecting on raising of cybercrime.<sup>108</sup> Various analytical reports of Russia LEAs indicate that organized criminal groups, including transnational ones, are more tended to utilize information technologies in their criminal activities.<sup>109</sup>

<sup>103</sup> Information provided in this table is collected from the official resource of the Ministry of Internal Affairs of the Russian Federation: <https://xn--b1aew.xn--p1ai/Deljatelnost/statistics>

<sup>104</sup> The figures of registered cybercrime cases include as cyber-dependant as cyber-enabled crimes.

<sup>105</sup> [https://www.ng.ru/economics/2020-09-10/1\\_7961\\_cybercrime.html](https://www.ng.ru/economics/2020-09-10/1_7961_cybercrime.html)

<sup>106</sup> See cases on: <https://iz.ru/tag/kiberataki>

<sup>107</sup> See [https://mvd.ru/upload/site120/folder\\_page/015/122/996/Gavrilin\\_Ch.1.pdf](https://mvd.ru/upload/site120/folder_page/015/122/996/Gavrilin_Ch.1.pdf) and <https://rg.ru/2020/10/23/eksperty-nazvali-tendencii-kiberprestuplenij-v-period-pandemii.html>

<sup>108</sup> [https://mvd.ru/upload/site120/folder\\_page/015/122/996/Gavrilin\\_Ch.1.pdf](https://mvd.ru/upload/site120/folder_page/015/122/996/Gavrilin_Ch.1.pdf)

<sup>109</sup> See "КОМПЛЕКСНЫЙ АНАЛИЗ СОСТОЯНИЯ ПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ И РАСЧЕТНЫЕ ВАРИАНТЫ ЕЕ РАЗВИТИЯ", prepared by the scientific-research institute of the MIARF, pp. 58-66; available at: [https://mvd.ru/upload/site163/document\\_text/Kompleksnyy\\_analiz\\_\\_original-maket\\_24\\_04.pdf](https://mvd.ru/upload/site163/document_text/Kompleksnyy_analiz__original-maket_24_04.pdf)

Darkweb is well developed in the Russian Federation<sup>110</sup> and offers a wide array of criminal opportunities: Drug Market,<sup>111</sup> trading with hacked personal data,<sup>112</sup> Crime as a Service (CaaS)<sup>113</sup>, etc. Independent Russian experts argue that there is a problem with underreporting of cybercrime in Russia and official statistic does not illustrate the real picture.<sup>114</sup> The Russian LEA sources also admit that cybercrime, especially when committed by organised criminal groups, is characterized by high latency.<sup>115</sup>

Russian authorities began paying utmost attention to cybercrime in recent years.<sup>116</sup> As officially and unofficially the LEA experts forecast an increase in cybercrime in the nearest future in the Russian Federation,<sup>117</sup> the government undertakes active measures for reducing the threats, including tailored awareness-raising campaigns for population<sup>118</sup> and LEA officers.<sup>119</sup> The authorities invest much in LEA capacity building for combatting cybercrime<sup>120</sup> and boosting government agencies' capabilities to deter cyberattacks.<sup>121</sup>

## 4. Ukraine

Similar to the neighbours, Ukrainian LEAs observe significant raise in cybercrime in recent years.<sup>122</sup> Cybercrime in Ukraine is generally perpetrated by internal and external threat actors. Soviet school STEM educational legacy serves in benefit for Ukraine as it affords a large number of professional workforce available for development Ukraine's cyber space and digital infrastructure but at the same time, it facilitates increasing numbers of illegal actors. If we take into account technical capabilities and resources which

---

<sup>110</sup> <https://www.pcmag.com/news/the-evolution-of-russias-dark-web>

<sup>111</sup> See for examples: <https://www.wired.com/2014/11/oldest-drug-market-is-russian/> and [https://medium.com/@Nethone/\\_russian-darknet-market-hydra-is-expanding-whats-the-threat-d0613d34a358](https://medium.com/@Nethone/_russian-darknet-market-hydra-is-expanding-whats-the-threat-d0613d34a358)

<sup>112</sup> See for example: <https://www.kommersant.ru/doc/4252853> and <https://www.theguardian.com/commentisfree/2018/jul/24/darknet-dark-web-hacking-forum-internet-safety>

<sup>113</sup> See for example: <https://www.bbc.com/russian/media-50091630>

<sup>114</sup> [https://www.ng.ru/economics/2020-09-10/1\\_7961\\_cybercrime.html](https://www.ng.ru/economics/2020-09-10/1_7961_cybercrime.html)

<sup>115</sup> See "КОМПЛЕКСНЫЙ АНАЛИЗ СОСТОЯНИЯ ПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ И РАСЧЕТНЫЕ ВАРИАНТЫ ЕЕ РАЗВИТИЯ", prepared by the scientific-research institute of the MIARF, pp. 58-65; available at: [https://mvd.ru/upload/site163/document\\_text/Kompleksnyy\\_analiz\\_\\_original-maket\\_24\\_04.pdf](https://mvd.ru/upload/site163/document_text/Kompleksnyy_analiz__original-maket_24_04.pdf)

<sup>116</sup> See <https://russian.rt.com/russia/news/753680-medvedev-kiberprestupleniya-rossiya> and <https://www.rbc.ru/politics/08/07/2020/5f059cc39a7947682fa1e789>

<sup>117</sup> See [https://www.gazeta.ru/tech/news/2020/05/30/n\\_14485027.shtml](https://www.gazeta.ru/tech/news/2020/05/30/n_14485027.shtml) and "КОМПЛЕКСНЫЙ АНАЛИЗ СОСТОЯНИЯ ПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ И РАСЧЕТНЫЕ ВАРИАНТЫ ЕЕ РАЗВИТИЯ", prepared by the scientific-research institute of the MIARF, p. 66; available at: [https://mvd.ru/upload/site163/document\\_text/Kompleksnyy\\_analiz\\_\\_original-maket\\_24\\_04.pdf](https://mvd.ru/upload/site163/document_text/Kompleksnyy_analiz__original-maket_24_04.pdf) and [https://www.gazeta.ru/tech/news/2020/05/30/n\\_14485027.shtml](https://www.gazeta.ru/tech/news/2020/05/30/n_14485027.shtml)

<sup>118</sup> <https://regnum.ru/news/society/3011728.html>

<sup>119</sup> <https://www.kommersant.ru/doc/4537640>

<sup>120</sup> <https://www.rbc.ru/rbcfreeneews/5dbc32589a7947dcb50ecbc9>

<sup>121</sup> <https://iz.ru/1033009/video/mishustin-pro-kiberprestupnost>

<sup>122</sup> <https://www.epravda.com.ua/publications/2018/01/15/633003/>

are far better in Ukraine than in other countries of the region, it can be implied that the internal dimension of Ukraine's threat sources is significant.<sup>123</sup> On the other hand, Ukraine is targeted by external threat actors far more actively than Georgia.<sup>124</sup> In recent years, Ukraine suffered massive Russian attacks on different spheres of social life such as banking, energy, healthcare.<sup>125</sup> Occupied territories Donetsk and Lugansk Oblasts provide safe ground for such external threat actors as some Russian Federation-based groups operating against Ukraine moved there.<sup>126</sup> There are alarming signs of the path of transnational organised groups in Ukraine's cybercrime statistics.<sup>127</sup> The most popular cybercrime in Ukraine is Cyber-fraud, illegal content and malicious software (cyber-attacks). Ukrainian Cyber-police has active stance toward cybercrime and is focused on not only investigation but on preventive measures as well. It utilizes some technological projects for crime prevention and easy reporting.<sup>128</sup> It also conducts proactive operations using ethical hacking means.<sup>129</sup>

## 5. European Union

Europol cybercrime statistics reflected in Europol IOCTA 2020<sup>130</sup> and ENISA Threat Landscape 2020<sup>131</sup> describes the wider EU cyber threat landscape, challenges and common characteristics. These two threat analysis reports reveal the key cyber threats targeting the EU Member States: ransomware, phishing and identity theft remain the most dominant threat. The amount of online child sexual abuse material is on the rise, the variety of payment fraud has been increasing as well, while Darkweb is still a source of numerous types of cybercrimes. Cyber-enabled crimes take new forms.

Reliability of hardware and software, as well as service providers, are a serious challenge for the EU countries as it is primarily related to cybersecurity risks and therefore, affects national security, business, and residents at the same time. For this reason, the EU seeks to establish a common certification mechanism for devices and services.

---

<sup>123</sup> [https://ccdcoe.org/uploads/2018/10/Ch13\\_CyberWarinPerspective\\_Kostyuk.pdf](https://ccdcoe.org/uploads/2018/10/Ch13_CyberWarinPerspective_Kostyuk.pdf)

<sup>124</sup> Interview with Georgian cybersecurity expert Giorgi Iashvili.

<sup>125</sup> <https://www.reuters.com/article/us-ukraine-cyber-exclusive-idUSKBN1JM225>

<sup>126</sup> [https://ccdcoe.org/uploads/2018/10/Ch13\\_CyberWarinPerspective\\_Kostyuk.pdf](https://ccdcoe.org/uploads/2018/10/Ch13_CyberWarinPerspective_Kostyuk.pdf)

<sup>127</sup> <https://www.kyivpost.com/technology/ukrainian-cyberpolice-dismantles-international-hacking-scheme.html?cn-reloaded=1>

<sup>128</sup> <https://www.coe.int/en/web/cybercrime/-/cybereast-interview-on-legislative-development-and-training-activities-on-cybercrime-in-ukraine>

<sup>129</sup> <https://112.international/article/cyber-police-what-are-ukrainian-virtual-cops-doing-25336.html>

<sup>130</sup> <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020>

<sup>131</sup> See ENISA report Threat Landscape 2020 – LIST of TOP 15 Threats, available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats>

The member states use different tools and techniques to combat cybercrime, but the most prominent measures taken on the strategic level are as follows: awareness of general public, public-private partnership and collaboration among state agencies, improvement of technical capabilities and training of investigators. European countries are set to increase dedicated cyber-security budget in 2021 to meet newly emerged challenges. In Austria, as an example, the vast majority of CIs started to allocate additional budget in IT security and introduced new defence measures, a huge step forward compared to the previous years. Even though the increased funding in technical and software capabilities in most European countries was driven by enactment of NIS Law and GDPR, the fact itself already positively affected mitigation of threats.

## 6. Lithuania

Managing and mitigating cyber threats is one of the top priorities for Lithuania considering the increased number of incidents taking place in its cyberspace. Analyses of the Lithuanian cyber-security situation shows that targeted attacks on CIs are a serious challenge, as in 2019 the country witnessed three times more cyber incidents compared to 2018.<sup>132</sup> Despite the active and mature approach of the government, public awareness in Lithuania remains low. This is identified as one of the factors facilitating the raise of cybercrime and thus negatively affecting statistics of cybercrime, as citizens do not report cyber incidents. Problems of reporting of cybercrime are also a great challenge for Lithuanian LEA. The categories of threat actors for Lithuania are similar to Georgia: External, internal, transnational organised criminal groups. Lithuania is the target of Advanced Persistent Threats (APT) groups. The most frequent cyber events in 2019 were Cyber threats to ICTs, Malware, Information gathering, Attempted hackings, CIs disruption.

Comparative analysis of EU's cyber threat landscape, as well as in the close neighbourhood of EaP region, reveals that Georgia shares the same denominators of cyber threats as the rest of the countries. This assumption of shared common threats is also reiterated by the prominent Council of Europe experts.<sup>133</sup>

---

<sup>132</sup> [https://www.nksc.lt/doc/en/NKSC\\_2019\\_EN.pdf](https://www.nksc.lt/doc/en/NKSC_2019_EN.pdf)

<sup>133</sup> Interview with EU expert, Besnik Limaj.

## CHAPTER V. GEORGIA'S HANDLING OF CYBERCRIMES AND ITS CHALLENGES

According to the Georgian legislation, the MIA bears the main responsibility to handle cybercrime as a part of the general policing function, including investigation of cybercrimes.<sup>134</sup> Formally, the MIA regional police departments – popularly known as criminal police – are authorized for policing cybercrimes.<sup>135</sup> The institutional capacity of the Georgian Police for handling cybercrime as a specific type of crime has been significantly developed since the formation of the Cybercrime Division of the CCPD at the MIA in 2012.<sup>136</sup> Currently, the Cybercrime Division represents the main arm of the Georgian police to deal with serious cybercrimes. It is also actively engaged in international cooperation for investigation of transnational cybercrimes.

Analysis of the legislation, official policy papers, analytical documents and the police newsfeeds evidence that the paradigm of the Georgian Police for handling of cybercrimes generally is built on responsive measures - taking steps for investigating cybercrimes and mitigating harms, while efforts of prevention are rare and fragmental. Independent experts also note that the police strategy for combatting cybercrimes is focused mainly on investigation; proactive and preventive activities are not envisaged as an important and systematic policy and operational direction.<sup>137</sup>

Although, when it comes to investigation, the official data demonstrates that the police response is not always effective. The low rate of resolution of cybercrime cases indicates problems of investigation capabilities of LEA. The table below shows the figures of registered and investigated cases by regions of Georgia.<sup>138</sup> It demonstrates how big the contrast in cybercrime reporting and investigation between CCPD and Tbilisi Police Department is in comparison with regional and local investigatory units throughout Georgia.

---

<sup>134</sup> See art. 16 of the law on police, available at: <https://matsne.gov.ge/en/document/view/2047533?publication=28>

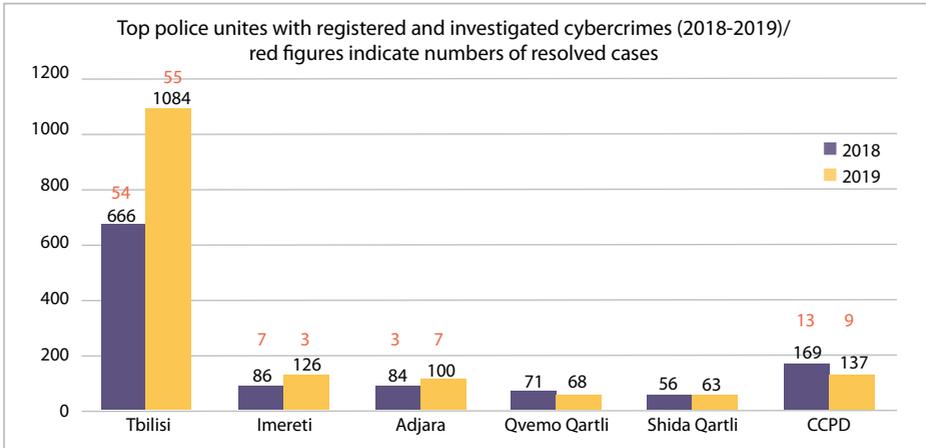
<sup>135</sup> Source: Ministerial Orders of the Minister of Internal Affairs adopting statutes of regional police departments.

<sup>136</sup> <https://police.ge/en/projects/kiberdanashauli/shinagan-saqmeta-saministros-mier-gankhortsielebuli-ghonisdziebebi>

<sup>137</sup> Interview with Georgian cybersecurity expert Irakli Lomidze.

<sup>138</sup> Source: draft of the National Strategy of Combatting Organised Crime.

**Table 8.** Registered and investigated cybercrimes in Tbilisi and Regions.



Currently, the challenges of Georgia’s cyber ecosystem having a direct influence on cybercrimes are much broader and go far beyond the MIA’s competences and capacities. Four main groups of mostly interconnected issues can be identified as challenging and negatively affecting the raise of cybercrime. These issues are regarding 1) institutional, policy and legal frameworks; 2) capacity and recourses; 3) cybercrime reporting, classification and information sharing; 4) public awareness and social engagement.

## 1. Institutional, policy and legislative frameworks

Cyber resilience is achievable only with “whole on nation” and “whole of government” notions. As the experience of developed countries illustrates, even very powerful and effective government authorities can’t cope with the problems of cybercrime alone, without the help of other government agencies and close collaboration with multiple stakeholders from the society. Within the government, it is required to systematically interconnect the work of the institutions with strategic, operational and tactical functions. Also, sustainable partnership schemes between the government, businesses and social groups are essential to maintain.

Institutionally, in Georgia cybersecurity functions are allocated between various government agencies including the MIA and DGA, therefore no clear strategic coordination framework exists to synchronise the government policy on a daily basis, to strengthen efforts of the public sector and enhance achieving of long-term policy goals.

The final draft of NCS indicates the absence of cybersecurity policy frameworks enabling effecting evaluation and enforcement mechanisms. The Georgian government sector CIs do not follow the requirements of the Georgian Law on Information Security. Just

only 6 institutions out of 38 are compliant with minimum security regulations and the rest is trying to postpone their portion of commitments from year to year in the course of already 8 consecutive years (after the adoption of the Information Security Act).<sup>139</sup> This fact clearly illustrates how insufficient enforcement of information on security requirements is even among key government agencies or government own businesses. While all CIs and the Georgian Government as a whole make emphasis on the importance of cybersecurity in public, there is little and scarce evidence that in practice, the government shows ownership and active endeavours to the development of the domain. These facts lead to the implications that there are challenges in the formation of coherent government cybersecurity policy. This conclusion is reinforced by the fact that national-level cybersecurity policy in the form of a nation-wide cybersecurity strategy has not been adopted since 2018, although the final draft has been submitted for the government approval.<sup>140</sup>

The existing legislative framework for information security needs a serious update.<sup>141</sup> The draft law introduced to the Parliament by its Defence and Security Issues Committee chairperson to improve legislation needs significant revision in order to make it compliant with the EU legal norms and best practice as several Georgian experts believe.<sup>142</sup> In addition, Georgian legislation regulating the work of the police is silent regarding issues of policing the cyber space.<sup>143</sup> The Georgian Police can act only based on regulatory frameworks of general policing functions which are not always appropriate, sufficient, helpful and effective. It is noteworthy, that more policing agencies worldwide are affording ethical hacking means for the prevention of crimes in cyberspace.<sup>144</sup> Therefore, policing is a very specific type of public administration that needs well-defined legal authority (including coercive or covert elements) with clearly prescribed boundaries and supervision mechanisms, especially when it relates to the sensitive human rights domain. The situation is also very challenging when it comes to special operational procedures and internal guidelines of the police directing the daily work of every policeman. The MIA has drafted Standard Operational Procedures on Handling the Digital Evidence, which specifies software programs and technical

---

<sup>139</sup> Information from presentation of Digital Governance Agency.

<sup>140</sup> <https://www.interpressnews.ge/ka/article/620063-keli-degnani-sakartvelos-mtavrobas-movu-codebt-daqovnebis-gareshe-moaxdinov-erovnuli-kiberusaprtxoebis-strategiis-da-samokmedo-gegm-is-ratipikacia?fbclid=IwAR1WzA6JDd8j1kclVQMzqqKLABf3YLQp9YyFjOr51UcDHeevQS28Yyey6h0>

<sup>141</sup> Interview with Georgian Cybersecurity Expert Giorgi Iashvili.

<sup>142</sup> [https://idfi.ge/ge/risks\\_and\\_challenges\\_of\\_the\\_draft\\_amendments\\_to\\_the\\_law\\_of\\_georgia\\_on\\_information\\_security](https://idfi.ge/ge/risks_and_challenges_of_the_draft_amendments_to_the_law_of_georgia_on_information_security)

<sup>143</sup> See the law on Police, available at: <https://www.matsne.gov.ge/en/document/view/2047533?publication=28>

<sup>144</sup> For example, Israeli police actively utilizes cyber units conducting active offensive operations in cyberspace. see. Nadav Morag, *Comparative Homeland Security. Global Lessons. Second Edition.* Hoboken, New Jersey, John Wiley and Sons. 2018, p. 338;

rules to be used when searching and seizing electronic evidence, but so far, this document has not been officially approved. General Prosecutor's Office of Georgia has developed general guidance on cybercrime investigation, but they do not address electronic evidence collection.

## **2. Capacity and Resources (workforce, technical equipment)**

Cybercrime threats are constantly sophisticating, growing and diversifying, volume and complexity of cybercrime increases. In these circumstances, cybercrime and cybersecurity authorities must continually adapt approaches to tackle them. It requires a continuous reformation process of cybercrime investigation and LEA should be one step ahead of criminals in order to move from the reaction process to prevention phase. Investment in cybercrime investigation technologies, tools and equipment are of great importance in order to provide an effective response to cybercrime threats.

Contrary to that, no specific budgets have been allocated to cybercrime and cybersecurity authorities for the implementation of national cybersecurity strategies and development of their capacity in the previous years, causing just ad-hoc performance of national-level cybersecurity activities.<sup>145</sup> Generally, financial resources are allocated in the budget of the MIA and other state agencies and are mostly dedicated to operational, day-to-day cybersecurity activities that limits county's capacity to perform strategic initiatives and its ability to be involved in other long-term development programs.<sup>146</sup>

Along with an insufficient number of cybersecurity specialists, the problem of qualification is also evidential. There is a high demand for cybersecurity specialists on the Georgian labour market, but existing resource does not match the criteria to fully satisfy this demand. Georgia's cybersecurity system is not sustainable without a team of qualified specialists in place, which possesses relevant knowledge and experience to prevent, mitigate and respond to cyber incidents.<sup>147</sup> The main challenge in workforce development is that the country lacks systemic and sustainable mechanisms in this field. The Georgian police mostly relies on training programs either organized by donor organizations or supported by LEAs or educational institutions of the partner countries. This approach was effective in the beginning when the country needed a rapid boost in the human workforce without its own relevant capacities. But now when already certain knowledge and experience have been accumulated and a sufficient number of Georgian professionals are available as trainers and educators, it is

---

<sup>145</sup> Interview with CERT.GOV.GE representative;

<sup>146</sup> Lack of financial support as a key obstacle is stated in the final draft of NCS;

<sup>147</sup> Lack of capacity of cyber specialists as a key obstacle is stated in the final draft of National Cybersecurity Strategy of Georgia

appropriate and affordable to develop cyber lab or cyber range to make the workforce development sustainable.

Due to the growing cybercrime challenges, the MIA has undertaken several steps to increase its human capital. For example, as a part of the structural reform in 2019, the staff of the Cybercrime Division increased by 30%. With the support of the US and European partners, as well as donor organizations, the cybercrime unit staff are constantly developing their skills and capacities. The technical equipment required for the cyber investigations of the division is also being actively improved.<sup>148</sup> As the number of cybercrimes increases, there becomes a shortage of qualified and high-profile cybercrime investigators who can deal with sophisticated crime scenarios and are skilled in handling digital evidence and digital investigatory technics. These valuable resources are thus allocated to more urgent and more serious cases, while most low profile, but much outnumbered cybercrime cases are not duly considered.

As it can be figured out from various speeches of the Minister of Internal Affairs Vakhtang Gomelauri before the Parliament of Georgia, the needs of capacity building of regional police departments are acknowledged by the MIA and a certain plan to address those needs was elaborated. The plan envisages the establishment of specially designated units for combatting cybercrimes in all regional police departments with properly trained police personnel. Such unit was already created within the Tbilisi police department.<sup>149</sup> Also, the MIA plans to undertake proactive measures in cyberspace for early identification and prevention of criminal activities.<sup>150</sup>

The situation with digital forensic is less challenging. Three forensic laboratories operating in Georgia provide digital forensic services to crime investigators. Forensic-Criminological Division of the MIA of Georgia provides forensic services to Georgian LEA on criminal cases, including facial recognition, digital media and computer forensics. One of the forensic labs is established at the SSSG and also provides services to the LEA officers. LEPL National Forensic Bureau provides independent expertise to public and private organizations and has three people dedicated to IT and computer forensic services. Therefore, the constant development of the capacity of digital forensic facilities is necessary to address the needs of LEA investigations in this rapidly developing sphere.

Finally, DGA also needs serious capacity building and allocation of additional financial, human and technical resources to implement its functions effectively. CERT.GOV.GE has seized operation of multiple cyber incident reporting tools due to unavailability of fi-

---

<sup>148</sup> "Government Report to Parliament on the implementation of the government program for 2019-2020" available at: [http://gov.ge/index.php?lang\\_id=geo&sec\\_id=458](http://gov.ge/index.php?lang_id=geo&sec_id=458)

<sup>149</sup> Source: Transcripts of the records of joint meeting of the parliamentary Legal Affairs and Defense and Security Issues committees 22.12.2020; also, transcript of the records of the parliament session 5.03.2021.

<sup>150</sup> *Ibid.*

nancial and human resources. This trend makes serious negative consequences on the sustainability of CERT's cyber incident handling capacity and puts CERT-LEA cybercrime cooperation at stake. Boosting the capacity of DGA and its CERT.GOV.GE directly impacts on the effectiveness of the government's efforts for the realization of proactive and preventive cybersecurity policy.

### **3. Cybercrime Reporting, Classification and Information Sharing**

Currently, there are three ways to report cybercrime to the police: 1) contact CERT; 2) go to the police station and fill the complaint 3) call 112 emergency call centre. The last two ways are traditional channels of communications of individuals with police. In many countries, police attempt to develop additional fewer formal opportunities to easy cybercrime reporting (for example various digital platforms and applications). Currently, in Georgia CERT represents such friendly and less formal platform which is not effectively utilised by LEA. CERT.GOV.GE is a trusted cyber authority among public-private stakeholders, it periodically hosts and shares incident information within Georgian Cybersecurity Forum and undertakes certain proactive measures. In this context, it is a key shortcoming that since 2012, CERT – LEA cooperation bears informal and ad hoc character. There is no formal platform established. Also, neither, rules and regulations for cyber incident information sharing are laid down in the legal document, nor information sharing standard is defined between CERT and LEA. Such formal cooperation gains utmost importance, especially when there is a problem of underreporting.

Common categorisation (taxonomy) of cyber incidents has not been developed within Georgian cyber authorities. CERT.GOV.GE follows ENISA model - "Reference Incident Classification Taxonomy". Mapping of different taxonomies undergone by ENISA shows that LEA can largely rely on CERT categorized cyber incident data for its own purposes - reported cybercrimes. There is a need for the development of "Common Taxonomy for the LEA agencies and CERT/CSIRTs".

The existing cybercrime reporting system does not allow to get a deeper classification of cybercrimes. The information under Article 284 (illegal access) that refers to crimes that have been committed without having more specific crime reporting data, i.e., specifying what type of cybercrime took place is not sufficient for analysis and planning of the police work. In Georgia, ransomware, for example, is not a separate cyber category, as the country maintains a general category for data breaches, based on cybercrime articles of the CCG. Having general categories for data breaches leads to the classification of problems, as different types of Cybercrimes fall into the same category. Providing statistical data based on calculation cyber-dependant crimes and considering only pure cybercrimes under criminal statistics, significantly limits the capacity of analysis and planning of the MIA

itself and other stakeholder agencies. Eventually, such approach is misleading for the GOG to elaborate proper policy and allocate sufficient resources for combatting cybercrimes. It has to be taken into account that there is an emerging trend of replacing conventional crimes with cyber-enabled crimes in the neighbourhood of Georgia.

Crime registration at the local police level maintains its own challenges as local police units (except Tbilisi and some other cities) do not have the expertise to assist a victim of cybercrime. Reporting cybercrime to a central authority from regions is an extra burden that sometimes victims do not want to take. Additionally, the information reported to local police may not find its way to national or central units, meaning LEA is unable to connect the dots on a national scale.

The exchange of information on cybercrime between public agencies, as well as within public and private sectors to combat cybercrime bears almost an informal character, it is ad-hoc and largely unregulated.<sup>151</sup>

There are some formal and informal mechanisms that enable basic cooperation between domestic actors and across borders to deter and combat cybercrime: The cooperation of ISPs and MIA is governed by the Memorandum of Cooperation. By signing this memorandum, the ten largest ISPs, the Office of General Prosecutor and the MIA agreed on the cooperation principles in the process of investigation of cybercrimes with the rights and responsibilities of the parties involved. Specialized contact points within the ISPs and LEA were designated to reduce the processing time of LEA requests<sup>152</sup>. There is a need to update the MoU, enlarge cooperation scope and modus operandi including inter alia some joint awareness-raising actions.

Importantly, in Georgia, there is no practice of publication of national strategic cyber threat situation analysis that will act as a key source on existing and emerging cyber-crime threats and precaution measures for stakeholders and general public.<sup>153</sup>

## 4. Public Awareness and Social Engagement

According to ITU, 68.85% of individuals in Georgia had access to the Internet in 2019. It is a dramatic increase in internet access if we compare this figure to the same indicator of 2010 (26,90%) and 2000 (0.48%)<sup>154</sup>. ITU data also shows that 75.8% of households in Georgia have Internet access at home.<sup>155</sup> Georgian National Communications Commis-

---

<sup>151</sup> Source: the draft of the National Cybersecurity Strategy;

<sup>152</sup> <https://www.coe.int/en/web/cybercrime/-ministry-of-internal-affairs-ge>

<sup>153</sup> <https://ncsi.ega.ee/>

<sup>154</sup> [https://www.itu.int/en/ITU-D/Regional\\_Presence/Europe/Documents/Events/2020/5G\\_EUR\\_CIS/5G\\_Georgia-final.pdf](https://www.itu.int/en/ITU-D/Regional_Presence/Europe/Documents/Events/2020/5G_EUR_CIS/5G_Georgia-final.pdf)

<sup>155</sup> <http://handle.itu.int/11.1002/pub/81550f97-en>

sion (GNCC)'s data of 2019 states that the number of mobile internet users in comparison with country population amounts to 93%, that is around 3,2 million people.<sup>156</sup>

Despite such impressive progress in boosting internet access, the majority of Georgian internet users are not properly aware of internet-related problems. The E-Readiness survey respondents stated that only 50% realized the importance of security and privacy and they paid attention to it, while less than 30% used any cybersecurity tools and solutions as such.<sup>157</sup> These figures demonstrate how irresponsive and unprepared the Georgian society tends to be towards cybercrimes. The Georgian private sector is absolutely free from regulatory standards in this domain, which plays a certain role in limited social activism in the process of building cyber resilience. The majority of businesses do not pay adequate attention to raise awareness, they rarely sponsor or provide any campaigns to contribute to awareness-raising campaigns for their workforce. Radio Liberty's Georgian service reported that a majority of Georgian local public servants, including high ranking officials, use Russia-based e-mail service.<sup>158</sup> This very alarming fact indicates how deep the problem of public awareness could be in the country in general. When educated and more or less informed civil servants utilize e-mailing system operating in the country undertaking hostile actions against their nation almost daily basis, it means that they don't take risks seriously. It can also be implied that the majority of ordinary citizens would approach this issue even more carelessly. As it was considered in the previous chapter, low public awareness regarding cybercrimes is a common problem in a close neighbourhood of Georgia as well.

DGA implemented various small projects to support the raising of awareness in recent years, while the Georgian police, well known for their active and large-scale social campaigns for popularisation of road safety or influencing against domestic violence, have not realized any significant program in this field. ISP and other private sector businesses, as well as various civil society organisations working on the informed citizenry and social education projects also do not show great interest to contribute to the improvement of social resilience. It seems that the GOG needs to take the lead and initiate decisive steps to address this very challenging problem.

---

<sup>156</sup> <https://www.comcom.ge/uploads/other/5/5671.pdf>

<sup>157</sup> IPM has implemented the E-Readiness study on the whole territory of Georgia in 2016 initiated by USAID/Tetra Tech ARD, in frames of E-Georgia Project.

<sup>158</sup> <https://www.radiotavisupleba.ge/a/ru---%E1%83%A1%E1%83%90%E1%83%AF%E1%83%90%E1%83%A0%E1%83%9D-%E1%83%A1%E1%83%90%E1%83%9B%E1%83%A1%E1%83%90%E1%83%AE%E1%83%A3%E1%83%A0%E1%83%94%E1%83%91%E1%83%A8%E1%83%98-/29981153.html>

### 1. Key Findings

- ✘ Cybercrime is still an emerging phenomenon in Georgia, its damaging potential is not fully exposed and the threat is not perceived properly either by the government or the society.
- ✘ Highly likely cybercrime remains underreported in Georgia as in many other countries of our region.
- ✘ The MIA is focused on pure cybercrimes and does not calculate cyber-enabled crimes under cybercrime statistics that leaves room for ambiguity.
- ✘ From the perspective of criminal justice, policy cybercrime still does not expose serious challenge to society as its share in general criminal statistics is not significant.
- ✘ In the context of national security, cybercrime is more dangerous than other crimes as it represents an instrument of transformation of external threats into serious problems of internal security.
- ✘ Georgian Police handle cybercrime generally in a reactive manner, with more focus on response - investigation and pursuit, lacking a comprehensive preventive approach.
- ✘ LEA has certain problems in investigation and digital forensic, especially, in the regions.
- ✘ Lack of coordinated government policy, mature engagement of the private sector and low public awareness in the light of digitalization of social life, increasing internet and ICT access are main factors affecting cybercrime statistics negatively.
- ✘ Transnational criminal activities expose little danger to Georgia cybersecurity nowadays, but it's predictable that GOCGs being an important part of transnational organized criminality, will increase their illegal activities in the digital space.
- ✘ Lack of sustainable financial support to develop key cybersecurity services and programs is observed.
- ✘ As main determinants affecting of raising cybercrime in Georgia are mostly generated through complex internal socio-economic and technological developments and external geopolitical processes and the GOG has limited capacity to influence significantly on most of those factors in a short-term perspective, it can be implied that in the nearest 5 years' period, the trend of raising cybercrime rates in Georgia will be maintained. Highly likely cybercrime would be increased approximately by 25-30% per year in comparison to 2020 rates and gradually, it will easily overcome 5% share of total criminal cases registered by the police in 2022.

## 2. Recommendations

### Recommendation #1. More preventive, proactive and protective policy

- ✘ Set up a comprehensive strategic agenda for cybercrime preventive measures. Georgia needs to develop not only reactive but also proactive measures for combating cybercrime.
- ✘ Change the approach of calculating cybercrime statistics to consider numbers of cyber-enabled crimes in total number of cybercrimes.
- ✘ Develop joint interagency task force from key government stakeholder institutions, equipped with strategic, operational and tactical tools, to unify efforts and undertake comprehensive and adequate measures for deterring external threats or mitigating the risks.
- ✘ Elaborate long-term strategy and action plan for combatting cybercrime, which will include capacity building, large-scale public awareness projects jointly organized by relevant government agencies (participation of the institutions responsible for implementing educational and youth policy is highly recommended).
- ✘ Draft and adopt legislative framework empowering the police for utilization ethical hacking and other proactive measures in cyberspace.
- ✘ Increase funding of cybersecurity dimension.

### Recommendation #2. Develop workforce and institutional capacity.

- ✘ Increase human and technological capacity of cybercrime investigators, especially at the regional level. Regular training programs with no gaps, as new sophisticated attacks require qualified people to deal with.
- ✘ Develop national training infrastructure for LEAs and security sector agencies to fill the gaps of human resources and facilitate professionalization of their personnel in cybersecurity, cybercrime investigation techniques and digital evidence.
- ✘ Increase efforts for participation in international exercises and trainings to increase international LEA cooperation with a special focus on combatting cybercrimes.
- ✘ Work more actively with LEAs of partner countries, international and regional law enforcement organizations in joint working groups and other platforms to detect activities of GOCGs in cyber sphere and be informed about possible threats.
- ✘ Create specialized cybercrime police units in every region of Georgia, equip them with special crime detection software and technical solutions that will increase early warning opportunities and increase other preventive technics.

- ✘ Equip and train enough police personnel properly for conducting tailored proactive policing measures countrywide.

### **Recommendation #3. Develop cyber culture.**

- ✘ Take active measures for public education and awareness, the empowerment of Georgian information society; reduce the success rate of many forms of cybercrime by educating individuals and organizations in recognizing criminal activity before they fall victim to it.
- ✘ Through various institutional frameworks achieve engagement of multiply government agencies having a large set of beneficiaries and active partnership with the private sector in the awareness-raising process to increase the outreach.
- ✘ Implement tailored educational campaigns for professional civil servants in cybersecurity, cyber hygiene and misinformation campaigns.
- ✘ Implement tailored and large-scale awareness-raising campaigns for the most vulnerable social groups.
- ✘ Share information about threats, best practices, specialized capabilities among stakeholders to build trust and demonstrate value for them.
- ✘ Raise awareness among decision-makers and senior management of LEAs to determine strategic priorities regarding cybercrime and electronic evidence;

### **Recommendation #4. Co-share resources between CERT and MIA**

- ✘ Temporary secondment - assignment, transfer of LEA professional in CERT in order to get a hand-on experience of CERT incident collection and reporting, classification approaches, together define procedural and organizational formalities. On the contrary, CERT representative can be shifted to cybercrime office in order to get more insight into procedural powers, investigation techniques and assist the process with technical cyber know-how. This advice is vastly promoted by ENISA, Council of Europe as a cooperative tool between cybercrime and cybersecurity authorities.<sup>159</sup>
- ✘ Adopt unified operational standards, develop the capacity of joint work; the experience of joint risk assessment teams of the MIA and the LEPL Revenue Service could be a useful example.
- ✘ Key steps required for information exchange between CERT and the police: Define a common taxonomy related to incidents and events in cybersecurity; Define an exchange standard to enable the sharing of information based on the taxonomy. Create statistics based on the information exchanged.

---

<sup>159</sup> Cooperation between CSIRTs and LEA: interaction with the Judiciary - <https://www.enisa.europa.eu>

### **Recommendation #5: Connect, communicate and collaborate**

- ✘ Strengthen formal and informal cooperation frameworks to combat cybercrime in order to build an effective and sound governance system:
- ✘ Elaborate and adopt legislative requirements for the exchange of information between public and private sectors.
- ✘ Foster cooperation between the MIA and ISPs.
- ✘ Develop a secure information sharing platform for the exchange of information on cyber-threats and incidents between cyber authorities.
- ✘ Undertake measures (including legislative amendments) to increase informed and responsible engagement of the private sector in strengthening the country's cyber resilience.

### **Recommendation #6: Develop Cybercrime Reporting Mechanism**

- ✘ Establish a cybercrime reporting centre, hotline, providing a central point of contact for citizens and businesses.
- ✘ Develop coordinated mechanisms within the public and the private sector allowing citizens to report cybercrime cases, including online fraud, cyberstalking, child abuse online, identify theft, privacy and security breaches, etc.
- ✘ Define common reporting methodology with written guidelines to broad stakeholder groups, including foreign counterparts.
- ✘ Launch awareness programs and communication campaigns to promote the regular use of reporting mechanisms by a wider community.
- ✘ Develop digital tools for cybercrime reporting.

## CHAPTER VII. CONCLUSION

Cyberspace is central to the functioning of the 21st-century societies. Cybersecurity encompasses borderless challenges, while responses remain overwhelmingly insufficient at both global and national levels. There are enormous gaps in both our understanding of the issue, as well as in the technical and governance capabilities required to confront it. States are inevitably required to develop defensive cyber capabilities, utilize proactive and preventive measures to be able to adequately defend their CIs, state and society. No state is capable to ensure security and resilience without close, timely and effective collaboration with all key cybersecurity players from public and private sectors internally, as well as internationally. Being timely and suitably aware protects targets from threats or gives more opportunities for risk mitigation and preparedness. Well-defined reporting is a source of real threat information which is the foundation for evidential policy planning. Effective cybersecurity-related information-sharing mechanisms are the foundation for evidence-based, actionable cybersecurity, and a success road leading to cyber resilience.

Threat information sharing in an actionable and timely manner is the state's execution of due diligence principle and responsible behaviour by the government towards the country at large.<sup>160</sup> Georgia should foster a culture of cybercrime/incident information sharing, build a trust-based relationship between the government and private players, facilitate cybercrime reporting from crime targets, incentivize companies and raise the confidence in the public in criminal justice response to cybercrime.

Finally, we believe that cybersecurity field is no more a "domain reserve" of the public sector, on the contrary, it affects every one of us and makes us a key player in the fight against cybercrime. Although there is no such thing as absolute security, there is no "all-mighty" solution to threats stemming from the use of ICTs. Georgia needs to analyse vulnerabilities, search for best solutions and country practices and come up with concrete policy decisions that will enable enhancement of state, industry or individual level cybersecurity. We strongly believe that the research paper will serve this purpose.

---

<sup>160</sup> Sharing is Caring: Collaborative Analysis and Real-Time Enquiry for Security Analytics - [https://www.researchgate.net/publication/333585739\\_Sharing\\_is\\_Caring\\_Collaborative\\_Analysis\\_and\\_Real-Time\\_Enquiry\\_for\\_Security\\_Analytics](https://www.researchgate.net/publication/333585739_Sharing_is_Caring_Collaborative_Analysis_and_Real-Time_Enquiry_for_Security_Analytics)



Research