ARTICLE:

PROBLEMS OF LEGAL REGULATION AND INVESTIGATION OF COMPUTER CRIMES IN GEORGIA

By **Ucha Zaqashvili**

Introduction

Computer crime in Georgia has provided fertile ground for hackers at the beginning their criminal activities, which in turn is facilitated by an absence of a unified security system, the lack of knowledge and ability of the law enforcement authorities in the high-tech field, and arguably the high level of latency of cybercrime in Georgia. When substantiating the insignificance of the problem in Georgia, many people often refer to official statistics. In order to make the research for my doctorate more thorough,[1] the author applied to the Administration of Ministry of Internal Affairs for the official statistics relating to the investigation of cybercrimes. The Ministry replied to my request with a letter dated 12 December 2007, reference 7/2/7-4772. It transpires that five cases have been registered in the years between 2001 and 2007, and two cases have been dealt with, in that the perpetrators were identified and convicted; one of these cases is discussed below. One further cybercrime was detected in 2008. As the final result, a total of six computer crimes have been registered in Georgia since 2001. Certainly, according to these data, there is practically no cybercrime problem in Georgia, but as readers of this Journal will be aware, is not difficult to invalidate the above opinion. With few exceptions, there are no Georgian monographs or research papers on the problem of computer crime, and no instructions and recommendations to improve the work of the law enforcement bodies to investigate cybercrime.

Against the background of numerous legal and practical problems in dealing with computer crimes in Georgia, the President of Georgia issued Decree No 215 of March 28, 2008 'On Signing the Convention on Cybercrime',[2] days before signing the Convention on Cybercrime on 1 April 2008.[3] On 9 January 2009, the 'United States-Georgia Charter on Strategic Partnership' was signed between Georgia and the United States of America in Washington, DC.[4] Section IV paragraph 2 of the Charter includes cooperation between the two countries on the issue of cybercrime:

> 'The United States and Georgia pledge cooperation to strengthen further the rule of law, including by increasing judicial independence. In this regard, the United States intends to provide assistance in this process, including training of judges, prosecutors, defence lawyers, and police officers. Through enhanced law-enforcement and judicial-branch relationships, we plan to address common transnational criminal threats such as terrorism, organized crime, trafficking in persons and narcotics, money laundering, and cybercrime.'

In August 2009, Christina Schulman stated in the *E-Newsletter on the fight against cybercrime* that among current programmes, the cybercrime project in Georgia was one of the most important projects aimed at assisting Georgia in developing a relevant policy in connection with the implementation of the Council of Europe Convention on Cybercrime.[5] This article will

[1] *The author is a candidate for a doctoral degree at Ivane Javakhishvili Tbilisi State University, Tbilisi, Georgia, with the following research title: "Problems of legal regulation and investigation of computer crimes in Georgia".*

[2] *Budapest, 23.XI.2001 ETS No 185.*

[3] *Work has already begun in Georgia to implement the terms of the Convention. On 29 September 2009, a workshop was held at the Ministry of Justice in Tbilisi with the Council of Europe on the practical issues to be addressed under the 'Project on Cybercrime in Georgia' – the programme is available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/2215_draft_agenda_ws_23Sep09.pdf.*

[4] *A copy is available at http://www.america.gov/st/texttrans-english/2009/January/20090109145313eaifaso.2139093.html.*

[5] *Cristina Schulman, 'Council of Europe measures for fighting against cybercrime', E-Newsletter on the Fight Against Cybercrime, Issue 2, August 2009, p. 35.*

review the problems of the legal regulation of computer crime, and the investigation of computer crime in Georgia.

The criminal regulation of cybercrime in Georgia

Chapter XXXV of the Criminal Code of Georgia is included in Book IX "Crimes against public security and order", and consists of articles 284, 285 and 286 under the heading "Computer crimes". One additional article stipulating criminal liability covers cyber terrorism (article 3241), which is included in Chapter XXXVIII (Terrorism) of the Criminal Code, which in turn is included in Book XI (Crimes against the State). Under the Criminal Code of Georgia, computer crimes are classified as minor offences (except cyber terrorism). Their objective elements are mainly material, but we may also deal with formally defined crimes as well.[6]

The offences under article 284

The unofficial translation of article 284 provides:

> Article 284. Unauthorized access to computer information
>
> 1. Unauthorized access to computer information protected by law stored in electronic computers, their systems or networks or on the machine carriers that causes the erasure, blocking, modifying or obtaining data, or disturbing the work of electronic computers, their systems or networks, as well as changing the International Mobile Equipment Identifier.
>
> shall be punishable with a fine, or by corrective labour for up to two years or imprisonment within the same term.
>
> 2. The same action performed by:
>
> a) a group of persons in prior agreement;
> b) the abuse of an official position;
> c) a person having access to electronic computers, their systems or networks,-
>
> shall be punishable with a fine, or by corrective labour for up to two years in length or imprisonment within the term from two to five years.
>
> 3. The action provided by Parts 1 or 2 of the current article that entail grave consequences is punished with a fine, or imprisonment within the term from two to five years.

The definition of the object of the crime is important. This provides for the correct classification of an action as a crime, so that it is possible to distinguish one crime from another and to correctly decide the issue of liability. The generic object of crime is the main basis of the system of the private part of the Criminal Law[7] As the chapter dedicated to computer crimes is included in the Book IX of the Criminal Code of Georgia – "Crimes against public security and order", it should be mentioned that the legislator has defined public security and order as the generic object of these crimes. Dr Katzman points out that the results of unauthorized use of information may vary: it may violate security of intellectual property as well as disclose information about the private lives of citizens, cause property damage, reputation damage, and the violation of normal process of production, amongst other things. The generic object of trying to prevent computer crime is the provision of public security and order, and the general object is the unity of all social relations for the lawful and secure use of information.

Dr Katzman associates the definition of direct objects with the headings of specific articles containing elements of computer crime.[8] Associate professor G. Mamulashvili specifies the privacy of the data stored in

[6] *In the Criminal Code of Georgia (which falls under the Romano-Germanic legal system), crimes are divided into formally defined crimes and materially defined crimes. Formally defined crimes are criminal actions that do not require a certain result to define them as completed crimes. For example, robbery is the crime of taking money or material values by threatening with a weapon. To charge a person with robbery, it is not necessary for a corresponding result to occur. The act will be considered completed immediately upon commitment of the action as stipulated by the offence. Materially defined crimes imply the existence of a certain result following the action, for instance, a murder. If there is no corpse, a person cannot be sentenced for murder if he only shot or threatened another with killing. In this instance, it is argued that materially defined crimes are also relevant.*

[7] *A. Gabiani, N. Gvenetadze, I. Dvalidze, N. Todua, M. Ivanidze and others, General Part of Criminal Law, (Tbilisi University Press, Tbilisi, 2004), p. 91.*

[8] *A. Katzman, PhD thesis "Computer crime", (Ivane Javakhishvili Tbilisi State University, Tbilisi, 2004), p. 35. In the Criminal Code of Georgia there are four elements to an offense:*

1 *The object of the crime that implies an object for the purpose of infringement upon which the crime is committed;*
2 *The subject of a crime implies a person who may commit a crime;*
3 *The objective aspect of crime implies the content of the criminal action;*
4 *The mental element of crime implies the perpetrator's attitude towards the action that has been committed, which includes direct intent, negligence, recklessness etc.*

the computer, that is, the property right to digital data,[9] as the direct object of the crime provided for in article 284, but the direct object of the offense may be the use of copyright material, for instance. The subject of the offense set out in article 284 is 'computer information' that is protected by law and which is contained in an electronic computer, its system or network.[10] The Criminal Code of Georgia does not provide for any clause about special objects, but it would be better if the Criminal Code of Georgia specifies a computer system as serving state interests as the object of special protection of a computer crime, in a similar way as that of the criminal laws of other countries.[11]

Applying the provisions of this article in practice may be difficult. To refer to unauthorized access to legally protected computer information (digital data), it is necessary to know what constitutes information in general, and what is meant by computer information. Information is a Latin word and means, in essence, 'acquainting', 'conveying' (in English, it is from the old French 'enformacion', 'informacion' and the Latin 'information-em'). There are many ways of interpreting information, and it is remarkable that the legal interpretation of an issue is impossible without a philosophical consideration of the meaning of 'information'. In philosophic literature, mainly attributive and functional concepts are used for defining information. Proponents of the first concept consider that information is an intrinsic feature of a material object, while others do not admit the existence of such information. There are many interesting opinions about this issue, but the legal interpretation of 'information' is the most important for the purposes of this article. From the legal point of view, information is data representing the subject of legal relations in the process of communicating (receiving, saving, processing, and transmitting) and may become the basis of the creation or termination of any legal obligation.[12]

It is possible that documents, databases, informational resources, and information arrays all contain information (digital data). Only confidential information is protected by the law. This means that an offense is only committed when a person obtains access to or modifies confidential information.

According to the current legislation of Georgia, the following areas are protected by law: state secrets (paragraph 1 of article 1 of the Law of Georgia "On State Secrets"); commercial secrets (article 272 of the General Administrative Code of Georgia), personal secrets, where what constitutes a personal secret is determined by the information, except as otherwise prescribed by the law (article 27 of the General Administrative Code of Georgia), and tax secrets pursuant to the Order of the Minister of Finance of Georgia "On approval of Instruction of compartmenting information containing tax secret and secret clearance"; this includes data about the tax payer from the moment the tax payer registers with the tax office, covering letters, orders issued for checking tax payers, tax inspection reports, letters of encashment, taxation files, and the tax payers' register.

The term "unauthorized" implies that the perpetrator acts without permission of the owner of the computer, its system or the network owner. The term "access" should be explained as a person's efforts to carry out certain actions and as a result, interferes or influences the process of processing information without authority. The action may be either simple – direct physical access to the computer, or technical – penetration into the computer network through the internet by means of various software tools. To prove unauthorized access, a causal relationship must necessarily exist between the act and the result. But it can be very difficult to establish such a link. For example, assume a perpetrator steals the password of a bank system by obtaining access to the system when physically located in Israel. Later, another person uses the password in Georgia and produces a forged credit card, which is then used by another person to undertake transactions in a number of shops. In this example, damage is incurred upon the lawful owner of the card, the bank and each shop. The causal relationship can be established in the following manner: the person who stole the password by obtaining access to the banking system without authority will have committed an offense as stipulated by article 284. The production and use of a forged card

[9] *M. Lekveishvili, G. Mamulashvili, N. Todua and N. Gvenetadze, Private Part of Criminal Law, Book 1, (Meridian, Tbilisi, 2005), p. 613.*

[10] *A. Katzman, PhD thesis, "Computer crime", (Ivane Javakhishvili Tbilisi State University, Tbilisi, 2004), p. 39.*

[11] *The term 'special object' can be described in terms of where, for instance, the punishment for murder is imprisonment for 15 years. It is clear that the object of this crime is the death of a human being, but if the legislator includes an article in which it is determined that the murder of a woman that is pregnant shall be punished with imprisonment for 20 years, it means that the legislator considers the life of a pregnant woman as an object of special protection. In this case, the author implies such object under the term 'special object'. For instance, obtaining unauthorized access to a computer system is punished with imprisonment of up to 2 years. However, it could be argued that where a person obtains unauthorized access to a computer system that is the state property must be punished more severely. In this case, the state owned computer system becomes the object of special protection of law.*

[12] *M. Tsatsanashvili, "Informational society and legal regulation of information", (Tech-Inform, 1999, page 26.*

represents another offense as provided for by article 210 of the Criminal Code.[13] Thus, although the chain of crimes began with the theft of the password, the person who obtained the password by obtaining access to the banking system without authority has not committed the illegal transaction in the shop.

The subjective aspect of the crime provided for by article 284 is expressed in direct intent, because the disposition of the Article is based on the term "unauthorized access". As the word "access" implies certain efforts to carry out certain actions to the detriment of the owner of the computer, its system or network, it means that this action can be committed only with direct intent.[14] However, in some cases there may be no direct intent in regard to the results of an action. For example, assume a person penetrates into a database in order to find out the flight time of the President of the country. Assume his purpose is neither to block, nor delete the information, nor do any other action that comes within the provisions of article 284 of the Criminal Code of Georgia. Assume the aim is to prepare and carry out a terrorist attack. It is difficult to classify this example as the crime set out under article 284. This is because the offense does not provide for obtaining unauthorized access for the purposes of committing other crime.

It might usefully be mentioned that before ratification of the Council of Europe Convention on Cybercrime, many countries associated a criminal act with the result of unauthorized access. By way of example, under the Council of Europe Convention and Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems,[15] article 2 provides as follows:

> Article 2 Illegal access to information systems
>
> 1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.
> 2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.

Some Member States of the European Union have implemented this article by imposing criminal liability for unauthorized access to information systems only if it results in damage of information. Latvia is one such example, as provided for under section 241 of the Criminal law:[16]

> Section 241. Arbitrarily Accessing Automated Data Processing Systems
>
> (1) For a person who commits arbitrarily (without the relevant permission or utilising the rights granted to another person) accessing an automated data processing system or a part thereof, if breaching of data processing protective systems is associated therewith or if significant harm is caused thereby,
>
> the applicable sentence is deprivation of liberty for a term not exceeding three years or community service, or a fine not exceeding fifty times the minimum monthly wage.
>
> (2) For a person who commits the same acts, if commission thereof is for purposes of acquiring property or if serious consequences are caused thereby,
>
> the applicable sentence is deprivation of liberty for a term not exceeding five year or custodial arrest, or community service, or a fine not exceeding one hundred times the minimum monthly wage, with or without confiscation of property.
>
> (3) For a person who commits the acts provided for in Paragraph one of this Section, if they are directed against the State information system,

[13] *The printing, spreading or use of forged credit or pay cards – Criminal Code of Georgia, Chapter XXVII "Crimes in Monetary-Credit System", Article 210.*

[14] *See Daniel Bilar, 'Known knowns, known unknowns and unknown unknowns: anti-virus issues, malicious software and internet attacks for non-technical audiences' Digital Evidence and Electronic Signature Law Review, 6 (2009) pp 123 – 131.*

[15] *OJ L69, 16.3.2005, p. 67–71.*

[16] *Adopted 17.06.1998, effective since 01.04.1999 [17.06.1998. likums "KriminĢllikums" ("LV", 199/200 (1260/1261)].*

the applicable sentence is deprivation of liberty for a term not exceeding eight years or a fine not exceeding one hundred and eighty times the minimum monthly wage.

[12 February 2004][17]

In a report from the Commission to the Council on article 12, it was noted that in Austria, criminal responsibility requires intent to perpetrate data espionage and to use the data obtained in order to make a profit or to cause damage; in the Czech Republic, criminal liability only occurrs where there is illegal access and where the data are subsequently misused or damaged, and in Finland, the requirement for criminal responsibility is that the data must be 'endangered'.[18]

Applying the elements of the offence

In this section, consideration will be given to the situation where a hacker has obtained access to the airport database to find out the President's flight schedule for the purpose of a terrorist attack on the President. Assume the hacker has obtained the flight schedule of the President, and also assume that the hacker mistakenly deletes this information and a number of files containing other information. Given the facts of such a case, it is correct to refer to the perpetrator's recklessness as a result of the unauthorized access. The perpetrator may not always have direct intent, but they may have been reckless or negligent.

Naturally, unauthorized access to a computer is unimaginable without direct intent, although a person can obtain access with authority, and then undertake actions that go beyond the authority granted to them.[19] This raises the question as to the nature of the action required to be proven for it to be classified under the Criminal Code of Georgia. Section 4 of article 10 of the Code provide that "an unintentional act shall be considered as a crime only if the relevant article of this Code so provides". Unfortunately, article 284 does not contain such clause,[20] although article 11 of the Code provides as follows:

Article 11. Liability for a crime of aforethought with attendant consequences

1. If a criminal law provides for an increase in the punishment where the consequences were not within the remit of the intent, then such an increase shall be permitted only if a person caused the consequences through negligence. Such action shall constitute a crime of aforethought.

2. Other qualifying features of the crime of aforethought shall be attributed to the accused only it was part of the intention of this person.

This interpretation can be useful only in regard to the aggravating circumstances as stipulated by paragraph 3 of article 284, which implies the grave consequence caused by any action stipulated by paragraph 2 and the criminal liability is increased for it. Thus, if a person

[17] *This is taken, with permission, from a paper by Stephen Mason, ' The implementation of Community regulations in national legislation: IT offences in the strict sense of the word and offences committed using IT' , prepared to support a talk by the author during a seminar entitled Investigation, Prosecution and Judgment of Information Technology Crime: Legal framework and criminal policy in the European Union. The seminar was held for members of the judiciary (judges and public prosecutors) specializing in dealing with cybercrime, organized within the framework of the European Judicial Training Network (with financial support from the Directorate-General Justice, Freedom and Security of the European Commission (2007 Criminal Justice Programme) and the Federal Public Service Justice (Belgium)) between Tuesday 25 November 2008 and Friday 28 November 2008 at the Hôtel Jean de Bohême, Durbuy, Belgium, and the full paper is available at http://www.stephenmason.eu /training-for-lawyers/judicial-training/.*

[18] *Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems 14.7.2008, /* COM/2008/0448 final */, paragraph 2.3.*

[19] *For a discussion in the US context, see Scott Eltringham, Editor in Chief, Prosecuting Computer Crimes Manual, Part 1 Computer Fraud and Abuse Act (Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, February 2007), available at http://www.justice.gov/criminal/cybercrime/ccman ual/index.html.*

[20] *Interestingly in the UK, the Computer Misuse Act 1990 (as amended by The Police and Justice Act 2006, s 36), provides, in section 3, for the following, which includes recklessness:*
3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
(1) A person is guilty of an offence if—
(a) he does any unauthorised act in relation to a computer;
(b) at the time when he does the act he knows that it is unauthorised; and
(c) either subsection (2) or subsection (3) below applies.
(2) This subsection applies if the person intends by doing the act—
(a) to impair the operation of any computer;
(b) to prevent or hinder access to any program or data held in any computer;
(c) to impair the operation of any such program or the reliability of any such data; or
(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.
(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.
(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—
(a) any particular computer;
(b) any particular program or data; or
(c) a program or data of any particular kind.
(5) In this section—
(a) a reference to doing an act includes a reference to causing an act to be done;
(b) "act" includes a series of acts;
(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

carries out actions that blocks, destroys or erases digital information as a result of unauthorized access to computer information protected by law, and these actions are committed under the circumstances stipulated by paragraph 2 of Article 284 and entail a grave consequence, and the perpetrator was reckless as to occurrence of such consequence, it will be considered as a deliberate crime. Where a person has committed the action set out in paragraph 1 of article 284, and acted recklessly or negligently as to the consequences, it appears that no deliberate crime has been committed, and his actions cannot be classified as a crime in accordance with article 284, because article 284 does not contain a clause for similar cases. The opinion provided in the comments to the "Private Part of Criminal Law" is also worth mentioning: "As for the subjective elements of computer crimes, the elements stipulated by articles 284 and 285 imply intent. Though there also may be recklessness as to grave consequence, but in a whole such crime shall be considered a deliberate crime".[21] Therefore, the action stipulated by article 10 of the Criminal Code of Georgia cannot be considered as a crime, except when a person was reckless as to the gravity of the consequences.[22]

The provisions of the Council of Europe Convention on Cybercrime tend to accentuate the subjective elements of the crime. For example, the damaging, deletion, deterioration, alteration or suppression of computer data cannot be committed unintentionally (this is stipulated by article 4 of the Convention):

> Article 4 – Data interference
>
> 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
>
> 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

This is similar to the offence set out in article 5 of the Convention on Cybercrime:

> Article 5 – System interference
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Aiding or abetting

The Convention on Cybercrime (article 11) and the Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (article 5) sets out an obligation to consider the issue of liability of persons attempting, aiding or abetting each of the substantive acts when a perpetrator acts intentionally. In this respect, the Criminal Code of Georgia follows the Convention, in that article 25 of the Criminal Code provides for liability of the immediate executor and accomplice (aider and abettor):

> Article 25. Liability of Perpetrator and Accomplice
>
> 1. Criminal liability shall be imposed upon the principal, aider or abettor only in respect of their own actions on the basis of joint illegal action, by taking into account the character and quality of the part that each of them played in the wrongdoing.
>
> 2. The criminal liability of the principal, aider or abettor shall be determined on the basis of the relevant article of this Code without reference to this article.
>
> 3. The criminal liability of the principal, aider or abettor shall be determined on the basis of the relevant article of this Code by reference to that article, except in those cases where principal, aider or abettor at the same time have been immediate co-executors.

[21] *M. Lekveishvili, G. Mamulashvili, N. Todua and N.Gvenetadze, Private Part of Criminal Law Book 1, (Meridian, Tbilisi, 2005), p. 613.*

[22] *An unofficial translation of article 10:*
Article 10. Unintentional crime
1. An act shall be deemed to be a crime of negligence if it is perpetrated through a presumption or recklessly.
2. An act perpetrated through presumption occurs where the person was aware that the action was foreseeable, and foresaw the possibility of the illegal consequence, but had an unfounded hope that he or she would avoid this consequence.
3. An act is committed recklessly where the person was aware that the action was foreseeable, and did not foresee the possibility that the illegal consequence might occur, although had he or she had given any thought to the consequences, they were able to foresee it.
4. An act committed recklessly shall be deemed to be an offence only if the relevant article of this Code so provides.

4. If the actions of the principal, aider or abettor involves actions that are relevant in respect of the wrongful act, then such actions shall give rise to the liability of the other principal, aider or abettor whose actions are not relevant in respect of the wrongful act if the latter principal, aider or abettor was aware of the actions of the other.

5. The personal feature, which is characteristic for the wrongdoing or the personality of one of the principals, aiders or abettors, shall be charged against the principal, aider or abettor who is characterized by that feature.

6. A person may be held responsible for complicity in a crime as an organizer, instigator or accomplice for participating in the crime as a special subject of the relevant crime prescribed by this Code.

7. If the perpetrator has not completed the crime, the accomplice shall be subject to criminal liability for the preparation of or complicity in the attempted crime. Criminal liability for the preparation of the crime shall be imposed upon the one who failed, due to circumstances beyond their control, to persuade other person into wrongdoing.

The Framework Decision also establishes liability for a crime committed by an organized group (article 7). Austria, Denmark, Finland and Portugal have not considered amendments connected with organized groups.[23] As for the Swedish legislation, a crime committed within an organized group is considered as an aggravating circumstance and is embraced by the term "grave crime".

Legal entities

Both the Council of Europe Convention on Cybercrime (article 12) and the Council of Europe Framework Decision (articles 8 and 9) provides for the criminal liability of a legal entity.[24]

Generally, the Criminal Code of Georgia stipulates liability for legal entities, but in the list of articles listing the criminal acts for which liability of legal entities may arise (article 1072 of the Criminal Code of Georgia), articles 284-286 are not mentioned, in contrast to article 3241 regarding cybercrime. This is one more inconsistency with the Council of Europe Convention on Cybercrime, and Georgian legislators will have to consider correcting this deficiency. Other countries have taken different approaches in Europe in respect to the issue of liability of a legal entity. In France and Estonia, it is considered that this issue should be governed by civil law, but Denmark, Finland and Portugal have not established criminal liability of legal entities.[25]

Section 2 of article 284 of the Criminal Code of Georgia has provided for aggravating circumstances where a person has obtained unauthorized access to legally protected computer information, which are as follows:

2. The same action performed by:
a) a group of persons in prior agreement;
b) the abuse of an official position;
c) a person having access to electronic computers, their systems or networks,-

Malicious code

Under paragraph 1 of article 285 of the Criminal Code of Georgia the following is punishable (the entire article is reproduced here):

Article 285. Production, use or circulation of detrimental electronic computer programs

1. The creation of detrimental electronic computer programs or the introduction of changes into current programs that result in erasing, blocking, modifying, copying information or disturbing the work of electronic computers, their systems or networks, as well as use or spread of such programs or machine carriers with them,-

shall be punishable by a fine or by corrective labour for up to three years in length or by a term of imprisonment similar in length.

2. The same actions entailed grave consequences are punished with imprisonment within the term from three to five years.

Paragraph 2 provides that the same action that gives

[23] *Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems 14.7.2008, /* COM/2008/0448 final */, paragraphs 2.6 and 2.7.*

[24] *For a translation of the Convention on Cybercrime by G. Lanchava and G. Ortoidze, (2008, Tbilisi) see http://www.cybercrime.ge.*

[25] *Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems 14.7.2008, /* COM/2008/0448 final */, paragraph 2.8.*

rise to grave consequences is an aggravating circumstance. There is no similar liability in the Council of Europe Convention on Cybercrime, which might be considered a deficiency of this document, rather than of the Criminal Code of Georgia. However, article 6 of the Convention provides as follows:

> Article 6 – Misuse of devices
>
> 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
>
> a the production, sale, procurement for use, import, distribution or otherwise making available of:
>
> i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;
>
> ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,
>
> with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
>
> b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
>
> 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

Article 4 of the Convention covers the establishment of criminal liability for damaging, deletion, deterioration, alteration or suppression of computer data. It can therefore be concluded that these articles taken together include the use of malicious software, although it is arguable whether the creation of malicious software is an independent crime and should be defined under a separate article in domestic laws.

From the analysis of disposition of article 285 of the Criminal Code of Georgia, it appears that if copying or modifying computer information is carried out by a program which does not damage the electronic computer, there will be no crime. Nevertheless, there are programs (for example, certain types of Trojan horse) which do not damage a computer but provide its creator with a control console to the system to which it will be sent and activated. Where the Criminal Code of Georgia provides that a perpetrator deals with digital data by means of malicious software, it appears that there is no criminal act under the provisions of article 285.

The offences under article 286

Article 286 of the Criminal Code of Georgia provides as follows:

> 1. The violation of an electronic computer, system or network operating rules on the part of a person who had access to electronic computers, their systems or networks, that results in deleting, blocking, modifying or copying legally protected computer information or causes considerable damage,-
>
> shall be punishable with a fine, or by socially useful works from one hundred and eighty to two hundred hours in length or by restriction of freedom for up to two years in length, by deprivation of the right to occupy a position or pursue a particular activity for the term not in excess of three years or without it.
>
> 2. The same action entailed grave consequences is punished with imprisonment within the term from two to four years.

A significant problem with the drafting of article 286 is that it provides for the establishment of criminal liability for the violation of certain rules, but it is unclear what is meant by the network operating rules, because such rules have not been established.

The offences under article 3241

Article 3241 of the Criminal Code of Georgia stipulates criminal liability for cyber terrorism:

1. Cyber terrorism, i.e. illegal seizure, the use or threat of use of cyber information protected by law, that creates the threat of giving rise to grave consequence, undermines public security, strategic, political or economic interest, perpetrated to intimidate the population or put pressure upon a governmental body,

   - shall bear the legal consequences of imprisonment ranging from ten to fifteen years in length.

2. The same action that has claimed a human life or has given rise to any grave consequence,

   - shall be punishable by prison sentences ranging from twelve to twenty years in length or by life imprisonment.

   Note: The legal person shall be punished with the winding-up or deprivation of the right to pursue activities and a fine for the crimes envisaged by the given article.

This article represents a formally defined crime, and will be considered as consummated immediately from the moment of illegal seizure or the use or threat of the use of information protected by law, although it is unclear why using information illegally acquired by citizen A on the part of citizen B may represent a computer crime. It would be easier to classify the act performed by A as unauthorized access (article 284 of the Criminal Code) and the act performed by B as a terrorist act (article 323 of the Criminal Code). Where it is proved that there was a relevant interconnection between them, it would be possible to punish A and B for participation in committing a terrorist act. It seems that the legislator has not analyzed how article 3241 can be applied, because it is difficult to define computer information "protected by law" under the Georgian legislation, and arguably it is better to punish a person who has committed cyber terrorism for committing a terrorist act stipulated by article 323 (Terrorist Acts) of the Criminal Code, rather than to attempt to detect elements of computer crime, than collect evidence and finally argue for a justified judgment of conviction. Unfortunately, the threat of using computer information protected by law may have no connection with obtaining access to computer information and committing computer crime in general. Even if it were not so, the legislator's purpose in regard to amending the Code by adding article 3241 seems strange, because paragraph 1 of article 323 provides as follows:

Article 323. Terrorist Act

1. Terrorist act, i.e. explosion, arson, application of arms or any other action giving rise to threat of a person's death, substantial property damage or any other grave consequence and undermines public security, strategic, political or economic interests of the state, perpetrated to intimidate the population or put pressure upon a governmental body,-

shall be punishable by prison sentences ranging from ten to fifteen years in length.

This article provides for the same purposes, and it does not matter how this act is committed, by what means and methods. Article 3241 accentuates a terrorist act committed by the seizure of computer information protected by law or its using or the threat of its use. Arguably, the latter is directly embraced by "or any other action" specified in article 323. Thus, the provisions of article 3241 do not necessarily help the authorities, because it is makes it more difficult to bring a cyber terrorist to justice. Another issue arises: if groups of people commit a terrorist act, and do so repeatedly, is considered an aggravating circumstance, the same aggravating circumstance ought to be for cyber terrorism as well. Also, the Note to article 323 provides for exemption from criminal liability where the person participating in the preparation of a terrorist act gives a timely notice to a governmental body or, by acting in another way, helps to prevent the terrorist act.[26] It is to be questioned as to why the same defence does not apply to enable a person to avoid liability for cyber terrorism, especially as the objects of

[26] *The note reads (unofficial translation): 'Note: Criminal liability shall be lifted from the person participating in the preparation of the terrorist act where they give a timely notice to a governmental body or acts otherwise, in such a way that their notice will help stave off the terrorist act, in circumstance where his or her action bears no other signs of criminal behaviour.'*

undermining and the goals of a terrorist act and cyber terrorism are identical.

Ratification of the Convention on Cybercrime

At the time of writing this article, work is underway in Georgia to ratify the Council of Europe Convention on Cybercrime. Legislative amendments are planned to be made to the Criminal Code of Georgia as well as the Georgian Code of Criminal Procedure. It is difficult to say how the articles of the Convention will be integrated into the Georgian legislation, but obviously it is expected that this process will overcome the deficiencies discussed above, and significantly improve the legal framework for dealing with computer crime. Against the background of the discussions in this article, it becomes evident that it is difficult to classify a crime under the criminal norms currently applied in practice. Moreover, no Georgian investigator, prosecutor or judge has any special knowledge or special instructions of how to interpret or apply a norm in relation to the cyber offences, and it remains very difficult to explain the gravity, character and even the "grave consequence" resulting from cybercrimes. This problem is demonstrated by an analysis of the Georgian investigative practice and the deplorable statistics of the law enforcement authorities.

Cyber attacks against Georgia

There is a significant problem facing Georgia at present – there is no unified cyber security strategy, few computer crime research centers, little coordination between specialists working in the high-tech field and internet providers – these and many other reasons facilitated the successful cyber attacks against Georgia in July and August 2008.[27] After similar attacks against Estonia in April 2007, a research center was founded in Georgia with the assistance of a number of member states of NATO (Germany, Slovakia, Latvia, Lithuania, Italy and Spain) which began its activities in August 2008. The problem with cybercrimes is indicated by the fact that the authorities in Georgia failed to undertake prosecutions for the cyber attacks that occurred against Georgian web sites in July and August.

Although article 22 of the Code of Criminal Procedure requires a prosecutor or investigator to undertake proceedings if there are grounds for doing so, it is not only necessary to identify the perpetrator of the attacks. The authorities also need the resources and knowledge to pursue the investigation against those responsible for the attacks. It can be considered that many practical issues, as well as the ill-defined state of the Criminal Code, is far from satisfactory in Georgia. The problem is, that the computer crime-related problems discussed in this article are arguably caused by the wrong approach to this issue in Georgia. In particular, computer crime has never been the subject of a thorough study by Georgian scientists. It is to be hoped that the recent cyber attacks against Georgia should provide an impetus for scientists working in this field to ensure their research is more profound, and for the state to change its cyber security strategy.

Computer crime investigations in Georgia

The investigation of computer crimes is a complicated problem for the Georgian law enforcement authorities, and the establishment of an anti-cybercrime division has not resolved the problems. This is illustrated in a case completed by the Judicial Division for Criminal Cases, Tbilisi Regional Court on 19 May 2004 with a judgment. Several persons were accused of committing actions stipulated by articles 180, 202, 210, 362, paragraph "a", section 2 and section 3 of article 284 of the Criminal Code of Georgia. For the purposes of this article, the investigation carried out in respect with the crime committed under article 284 will be considered, and the evidence obtained to prove the offence will be reviewed.

The judicial decision of the Tbilisi Regional Court of 19 May 2004 (case No 1/a-74)

This was a criminal action of Z. Tsinadze, Sh. Gogua and R. Manasherov.[28] It was expressed as follows (the facts are taken from the judgment):

> Joint Stock Company (JSC) "IntellectBank" and JSC "Bank of Georgia" had concluded MasterCard credit card service agreements with casinos registered and operating in Georgia – Casinos "Adjara", "Flamingo", "Aragvi", "Victoria", "Europe" and other economic entities under which card transactions were carried

[27] *For more information about the attacks, which preceded the physical invasion of Georgia, see the two reports entitled ' Russia/Georgia Cyber War– Findings and Analysis' , Project Grey Goose: Phase I Report (Project Grey Goose, 17 October 2008) and ' Project Grey Goose Phase II Report: The evolving state of cyber warfare' (March 20, 2009 greylogic).*

[28] *Z. Tsinadze was arrested pursuant to paragraph A part 2 Article 284 for the crime he committed under Part 3 of this Article. R. Manasherov, who was suspected of committing the same action, was found not guilty, but he was given a conditional sentence because of other criminal actions committed during his activities in the criminal group mentioned in the case. The remaining members of the group also went to trial (Judgment of Tbilisi City Court, file No 1/a – 74, May 19, 2004, page 83-85).*

out via point of sale terminals installed in each organization. Corresponding amounts were reimbursed to the legal entities by JSC "IntellectBank" and JSC "Bank of Georgia" from the funds transferred under the auspices of MasterCard.

Between September and October 2002, Georgian citizens Z. Tsinadze and R. Manasherov, Israeli citizen L. Zaitpudin and another unidentified person who was in possession of a forged identification document in the name of L. Mosashvili (obtained by prior arrangement for the purposes of unlawful misappropriation of property), intended to open card accounts at the Georgian banking institutions to receive MasterCard credit cards. Their intention was to illegally obtain access to computer information protected by law, and then unlawfully obtain and use information containing bank secrets, and authorize the transfer of credit amounts from foreign bank accounts into the credit cards issued to them, and then misappropriate the money by means of computer manipulation – "hacker operations", and to print forged credit cards and to misappropriate money from legal card owners by using them at non-banking facilities.

To execute the criminal act, Z. Tsinadze, by prior arrangement with other members of the group, received a MasterCard credit card from JSC "IntellectBank" on the basis of an agreement dated 7 November 2002. On the same day, Z. Tsinadze received two credit cards from the MasterCard system at the JSC "Bank of Georgia".

Simultaneously, Z. Tsinadze, R. Manasherov, R. Zaitpudin and L. Mosashvili decided to purchase computer equipment that would provide connection to the internet. The intention was to obtain illegal access to computer information protected by law, and to collect and use secret bank information for the purposes of their scheme to steal money. For this purpose, with the help of a friend of Z. Tsinadze, O. Alphaidze, they became acquainted with A. Dzidziguri, who had been working as a typesetter on the newspaper *Akhali Versia*. Dzidziguri had a good knowledge of computer equipment and was able to arrange, install and operate computer networks. A. Dzidziguri purchased two units of computer equipment for this purpose, and installed them in a house rented by L. Zaitpudin located in Chavchavadze Street.

After completion of all preparatory works, L. Zaitpudin offered to assist A. Dzidziguri in crediting amounts from foreign banking institutions to Georgia via the internet and printing forged credit cards, but the latter refused this offer of help. Nonetheless, Z. Tsinadze, R. Manasherov, L. Zaitpudin and a certain L. Mosashvili managed to obtain access to computer information protected by law and obtained data containing bank secrets of a number of foreign institutions reflected in the networks identified with the aid of other unidentified persons. They then repeatedly credited US$98,728.40 (by non-bank transfers) from various US facilities into the MasterCard credit card owned by Z. Tsinadze at JSC "IntellectBank" from 25 November to 11 December 2002 via the internet.

Z. Tsinadze then proceeded to cash US$2,000 at two ATMs of JSC "Bank of Georgia" on the next day (26 November 2002), although Z. Tsinadze and his accomplices failed to cash the remaining amount, because JSC "IntellectBank" refused to cash the amounts and blocked their credit card on the grounds that the credit operations were carried out as a result of forged transactions. The conspirators could not cash the amounts credited into the credit cards from banking institutions as a result of the forged transactions. This meant that the perpetrators changed the form of their criminal action, and decided to print forged credit cards of the MasterCard system which could be used at non-banking institutions such as casinos, supermarkets and other trade facilities.

L. Zaitpudin subsequently illegally purchased and brought to Georgia special equipment which was used for changing and falsifying the magnetic field for credit cards of the MasterCard system. At the same time, Z. Tsinadze disclosed his intent to Sh. Gogua, and involved him in the criminal activities. The perpetrators systematically printed forged credit cards using the credit card printing equipment,

collected information containing bank secrets by obtaining illegal access to computer networks, and changed the record of the magnetic field using this information. They entered the credit card numbers of those foreign citizens in whose name certain amounts of money were deposited at relevant banking institutions in the magnetic field of the credit cards issued by JSC "Bank of Georgia" and JSC "IntellectBank" in the name of Z. Tsinadze and L. Mosashvili. The perpetrators fraudulently used the forged credit cards at various facilities after which they misappropriated large amounts owned by legal holders of these cards.

Initially, criminal proceedings were instituted based on these facts on 28 February 2003 under articles 210 and 180 of the Criminal Code of Georgia. The grounds for the proceedings were based on the fraudulent misappropriation of funds by forged credit cards. Those investigating the crime arrested the suspect Z. Tsinadze and seized forged credit cards from him.

The investigation then led towards it being linked to a computer crime after receiving a letter from the International Legal Service[29] on 13 June 2003 informing the investigators that the US Federal Bureau of Investigation was investigating the illegal transactions with credit cards, and requested the authorities to provide relevant information regarding the credit card of the MasterCard system issued by JSC "IntellectBank" (the credit card number was also specified in the letter), the identity of the person in whose name the card was issued, the list of amounts deposited into the card, the location of withdrawal and the amount of money withdrawn.

On 17 June 2003, Georgian law enforcement agencies received a letter from US FBI investigator M. Kirbins, stating that the FBI was carrying out an investigation on the case of yet unidentified persons in Salt Lake City who stole credit card numbers from an American company "IronGate" (unfortunately, no specific information is provided in the text of judgement about the company "IronGate" apart from its name). These persons illegally penetrated into computer system of the internet company, copied the card-related information, and credited the amounts into their own credit cards accounts. One of the credit cards was issued by JSC "IntellectBank" in Georgia. The Federal Bureau of Investigation requested the authorities to provide information about this investigation, together with the MasterCard credit card issued by JSC "IntellectBank" (the credit card number was also specified in the letter).[30]

The Georgian investigators provided this information to the American investigators on the following day. By that time, the investigation had established that the credit cards requested by the FBI belonged to Z. Tsinadze. On 15 July 2003, the Georgian investigators sent a letter to M. Kirbins informing him of the detention of the suspects R. Manasherov and Z. Tsinadze, and asked him to share his experience in computer technologies and requested assistance. On 15 September 2003, the Georgian investigators again wrote to M. Kirbins informing him that the General Prosecution Office of Georgia was investigating a criminal case of fraudulent misappropriation of property as a result of printing and using forged credit cards and obtaining information from computers. The letter contained a request for assistance, provision of information about the credit cards opened in Georgia and into which suspicious amounts were deposited by means of the hacker operations. It is noteworthy that M. Kirbins did not reply to any of these letters. This is confirmed by an explanation made by one US Embassy employee on 30 October 2003.[31]

The law enforcement agencies were provided with the grounds to investigate the case under article 284. Although further evidence was necessary, the perpetrators were directly accused of the crime stipulated by article 284 of the Criminal Code, together with other crimes in the indictment dated 3 November 2003. The only thing the investigators were certain of was that a certain A. Dzidziguri installed computer equipment on behalf of the perpetrators. This is established from the interrogation protocols of A. Dzidziguri.[32]

The investigation of computer crimes is distinguished by a number of specific characteristics that exceed the knowledge of an investigator having a standard education in law. From the detailed study of this case, it is evident that the investigators classified the action under article 284 without any legal grounds. Paragraph 1 of article 284 provides that 'Unauthorized access to

[29] *'The International Legal Service' is mentioned in the text of the judgment and no other information is provided about this entity. It is assumed to be the Ministry of Foreign Affairs of Georgia, because the letter could have reached the investigation via this Ministry.*

[30] *Investigative practice of the General Prosecutor's Office, file number 1a-74, vol.4, pp. 93-95.*

[31] *Investigative practice of the General Prosecutor's Office, file number 1a-74, vol.5, p. 175.*

[32] *Investigative practice of the General Prosecutor's Office, file number 1a-74, vol.4, pp. 174-184.*

Although it is almost six years since the investigation of this case, it remains difficult to find an investigator in Georgia who has the capacity to conduct a proper investigation.

computer information protected by law stored in electronic computers, their systems or networks or on the machine carriers that causes the erasure, blocking, modifying or obtaining data, or disturbing the work of electronic computers, their systems or networks', and this means the investigators were under an obligation to establish the following facts: unauthorized access to computer information, system or network; the date and time of this took place; the place of access to the system or network; the reliability of the means of protecting the computer information; how the accused gained illegal access; the amount of loss incurred, and the circumstances contributing to the crime.

In this case, those investigating the crime should have requested, at the very minimum from the American company "IronGate", the runtime journal, list of IP addresses recorded in their server, and technical data relating to protecting the information stored on their computer to establish the fact of illegal access to their computer information, system or network. At the same time, the investigators should have become interested in the whereabouts of the computer equipment used by the perpetrators, and if found, they should have inspected and searched it together and with the assistance of digital evidence specialists, to establish whether it was possible to obtain access to the computer or networks that were attacked from these computers.

The investigators should have established whether the perpetrators had any e-mail addresses and if such existed, they should have checked the incoming messages on the basis of the judge's order, because it is possible that the criminals did not steal the credit cards themselves by means of unauthorized access, but received them from other persons, especially when there was evidence that L. Mosashvili was receiving the printable credit card details from international telephone calls. This fact is established from the protocol of additional interrogation of A. Dzidziguri.[33] The investigators failed to follow up the long distance calls, although such evidence had a great importance for the investigation of the case. The investigators should also have identified the telephone number and the internet service provider through which the perpetrators were connected to the internet.

From the letter of M. Kirbins, is becomes evident that the perpetrators were using numbers of credit cards stolen from "IronGate" for printing forged cards. Apart from this, the judicial records include a letter from an American company called First Data Corporation, which is attached to the case, which confirms that a total of US$98,000.00 was deposited to the credit card of Z. Tsinadze between 21 November 2002 and 9 December 2002, and which was stolen, although neither this fact nor any other evidence in the case disclose the identity of the immediate executor of the unauthorized access, the place and date and time of the unauthorized access, etc. This meant that the available information was not sufficient to accuse a person of committing an action under article 284. The investigation should have requested relevant information from the affected company first, and then should have conducted sufficient checks to ensure the information could be relied upon.

Although it is almost six years since the investigation of this case, it remains difficult to find an investigator in Georgia who has the capacity to conduct a proper investigation. The discussion in this article demonstrates the lack of preparedness of Georgian law enforcement bodies to deal with cybercrimes, and this represents the most significant problem in dealing effectively with computer crimes in Georgia, together with the lack of a sound legal framework.[34]

[33] *Investigative practice of the General Prosecutor's Office, file number 1a-74, vol.4, pp. 252-257.*

[34] *Arguably, some police forces in the United States of America have proved to be as inept in handling cases dealing with digital evidence, for which see the in-depth analysis of State of Connecticut v. Julie Amero (Docket number CR-04-93292; Superior Court, New London Judicial District at Norwich, GA 21; 3, 4 and 5 January 2007) by Stephen Mason (gen ed), International Electronic Evidence (British Institute of International and Comparative Law, 2008), pp xxxvi–lxxv).*

Conclusion

Based on the analysis of problems covered by this article, several important problems of dealing with computer crimes are outlined. One of the primary issues among them is the problem of the legal regulation of computer crimes. Against this background, it becomes increasingly apparent that Georgia needs to consider ratifying the Council of Europe Convention on Cybercrime swiftly. In addition, it is necessary to extend the borders of international cooperation and accelerate the training of digital evidence specialists for a future Computer Crime Division.

Ucha Zaqashvili became interested in computer crime in 2003 when stealing special passwords to use the internet free of charge was very popular in Georgia, and began working on his doctoral thesis regarding problems of legal regulation and investigation of computer crime in Georgia at Ivane Javakhishvili Tbilisi State University in 2006.

uchazaqashvili@yahoo.com

