AGORA International Journal of Juridical Sciences, www.juridicaljournal.univagora.ro
ISSN 1843-570X, E-ISSN 2067-7677
No. 1 (2014), pp. 29-34

HACKING AND COMPUTER CRIMES COMPUTER FRAUD – A COMPARATIVE LOOK AT THE NEW CRIMINAL CODE AND THE CRIMINAL CODE OF THE REPUBLIC OF MOLDOVA

A. T. Drăgan

Alin Teodorus Drăgan
Faculty of Juridical Sciences
"Vasile Goldiş" Western University of Arad
E-mail: alinteodorus@yahoo.co.uk

Abstract

Hacking involves the attempt to compromise the security of a computer system in order to gain unauthorized access. In the course of time it has turned out that the Internet is a vulnerable system, and this has generated a framework for criminal activities, resulting in the emergence of new crimes, among which computer fraud.

Keywords: *computer system hacking, computer fraud*

Introduction:

Cyber criminals elude the physical limitations that govern real-world crimes. The classic police model based on the principle that law enforcement bodies must react effectively and promptly to a crime, is less efficient against online crimes, because, in these cases, the police response usually begins long after the cyber crime was successfully carried out.

Hacking

Hacking is a complex task that requires a high level of technical knowledge. Usually it does not pay for a hacker to make the effort of penetrating a private home computer. Real hacking is typically done on computers that are likely to include the personal data of a lot of people, such as those of banks, databases of corporations, hospitals, schools, etc.

The term "hacking" is used very frequently, in fact, it is overused. Many individuals call themselves hackers even if they are not. In the world of hacking, the word "hacker" only refers to those who try to find vulnerabilities in different systems for research purposes. "Cracker" is the person trying to exploit the vulnerable parts of a system for malicious purposes. However, for the general public, as well as for most officials, the distinction has been lost[1].

Many in the hacking community object to the use of the term "hacker" in the media in order to denote illegal computer intrusions. In the hacking community a hacker is the one doing experiments on an information system in order to learn more about it.

Hackers are classified in a variety of groups, of which we will mention only a few.

The white hat hacker does not carry on illegal activities, he only learns about various information systems and seeks their vulnerabilities in order to subsequently provide security programs that protect the systems from illegal penetration.

The black hat hacker carries on illegal activities; these are the people who are usually associated with computer crimes. This term is synonymous with the word "cracker". Usually when the media talk about hacking, the reference is actually to black hat hackers.

The grey hat hacker is a combination of the white hat hacker and the black hat hacker. The best way to describe this class of hackers is by calling them opportunistic. If a grey hat

[1] Chuck Easttom and Det. Jeff Taylor, *Computer Crime, Investigation and the Law*, Course Technology, a part of Cengage Learning PTR, Boston, 2011, p. 10

hacker searches a target on the Internet and manages to gain access to a computer, he will notify the system owner[2].

There are numerous ways in which hackers manage to compromise an information system, including by finding a vulnerability in the operating system which can be exploited, denial-of-service attacks, or the so-called DOS, spamming, etc.

However, one must understand that hacking is not an easy task. Although many films have made it look like a hacker can gain access to highly reliable information systems within minutes, this is simply not true. Hacking is very similar to burglary: the safer the target, the more skill and time it will require for infiltration. A clever hacker will need a complete understanding of operating systems, information networks and security countermeasures.

Computer fraud in the new Criminal Code and in the Criminal Code of the Republic of Moldova

Legal content

As regards *computer fraud*, this criminal offence is provided for in Art. 249 of the new Criminal Code. This offence is reproduced without any significant changes from Law No. 161/2003 – only the penalty change, being diminished. In its turn, this special law merely reproduced the text of Art. 8 of the European Convention on Cyber Crime. Thus, according to Art. 8 of the Convention, regarding computer fraud, each Party should adopt legislative measures and other measures that are necessary to criminalize as an offence, under their domestic law, the act of intentionally and unlawfully causing a patrimonial damage to another person:

a) by any input, alteration, deletion or suppression of computer data;

b) in any form that affects the operation of an information system, with a fraudulent or wrongful intent to obtain without right an economic benefit for themselves or for another person.

With a view to noticing the similarities, according to the provisions of the new Code, a computer fraud consists in "the input, modification or deletion of computer data, restriction of access to such data or the hindrance in any way of the operation of a computer system in order to obtain a material benefit for oneself or for another, if damage was caused to a person".

In other words, computer fraud involves the input, alteration, deletion or superimposition of data or computer data or any other intrusion that might result in an influence on the outcome, thereby causing an intentional material or economic loss, the perpetrator seeking a patrimonial advantage for themselves or for another[3].

As regards the Republic of Moldova, computer fraud is regulated in Art. 260 Criminal Code. This article states that computer fraud means "the input, modification or deletion of computer data, restriction of access to such data or the hindrance in any way of the operation of a computer system in order to obtain a material benefit for oneself or for another, if these actions caused large-scale damages".

According to Art. 126, para. (1) of the Criminal Code of the Republic of Moldova, "extremely large-scale and large-scale damages are the value of goods that have been stolen, acquired, received, manufactured, destroyed, used, transported, stored, sold, passed across the customs border, the value of the damage caused by a person or a group of persons which, at the time of committing the criminal offence exceeds 5000, respectively 2500 conventional units of fine".

---

[2] Robert Moore*, Investigating high-technology computer crime, second edition*, Elsevier, 2010, p. 25

[3] Alexandru Boroi, *Drept penal. Parte specială, Conform noului Cod penal*, Ed. C.H.Beck, București, 2011, p. 230 (*Criminal Law. Special Part, According to the New Criminal Code*, C.H.Beck Publishing House, Bucharest, 2011, p. 230)

According to the legislation of the neighbouring country a fine is "a pecuniary penalty applied in the cases and within the limits provided by this Code. The fine is set in conventional units. The conventional unit for the fine is equal to 20 Lei".

So, in the case of computer fraud, the Criminal Code of the Republic of Moldova requires that at the time of committing the criminal offence the damage value should exceed 50,000 MDL (Lei of the Republic of Moldova), i.e. 14,000 RON (Romanian Lei).

We can see that unlike our criminal code, wherein the value of the damage does not matter, all that is needed is to prove that the patrimony of the aggrieved person has suffered a decrease as a result of the offence committed by the offender, the criminal code of the Republic of Moldova requires that the damage caused should be on a large scale.

Pre-existing conditions

A. Object of the criminal offence

a) The special juridical object is represented by the social relations that protect the security and reliability of assets represented or managed through information systems (electronic funds, deposits, electronic home banking, computerized control of stocks, accounts, automated desks that can be manipulated) or other instruments which may have consequences on property legal relations and on those relating to confidence in the security and reliability of the transfers performed[4].

b) The material object is the material entity (hard disk drive, CD, DVD, memory stick, etc.) on which the computer data are stored. In a broader sense, the material object is the entire information system[5].

According to Art. (1) of the Council of Europe's Convention on Cybercrime, a computer system means any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of data. Such a system may include data inputs, outputs or storage capabilities, may work alone or be connected to a network or other similar devices.

The convention also defines computer data as any representation of facts, information or concepts in a form suitable for processing in a computer system including a program that may cause a computer system to perform a function.

B. Subjects of the criminal offence

a) The active subject of this crime may be any natural or legal person, but in practice, manipulations are most often found to be committed by employees or officials or people with advanced knowledge in the field of computers[6]. The active subject might be even one of the employees of a trading company who should oversee the smooth running of the computerized management systems, in which case his discovery becomes a lot more difficult. Criminal participation is possible in all its forms (as an accomplice, co-perpetrator, instigator).

Under the Criminal Code of the Republic of Moldova the active subject of the criminal offence may be any natural person who has reached the age of 16 years.

---

[4] Alexei Barbăneagră, Gheorghe Alecu, Viorel Berliba, Vitalie Budeci, Trofim Carpov, Valeriu Cușnir, Radion Cojocaru, Alexandru Mariț, Tudor Popovici, Gheorghe Ulianovschi, Xenofon Ulianovschi, Nicolae Ursu, Victor Volcinschi, *Codul penal al Republicii Moldova: Comentariu*, Tipografia Reclama, Chișinău, 2009, p. 576 (*Criminal Code of the Republic of Moldova: Commentary*, Reclama Printing House, Chisinau, 2009, p. 576)

[5] Vasile Dobrinoiu, Mihai Adrian, Mirela Gorunescu, Maxim Dobrinoiu, Ilie Pascu, Ioan Chiș, *Noul Cod penal comentat*, Volumul II-Partea specială, Ed. Universul Juridic, București, 2012, p. 330 (*The New Criminal Code Commented*, Volume II – The Special Part, Universul Juridic Publishing House, Bucharest, 2012, p. 330)

[6] Ioana Vasiu, Lucian Vasiu, *Informatică juridică și drept informatic*, Ed. Albastră, Cluj, 2009, p.144 (*Legal Information Technology and Information Technology Law,* Publishing House: Ed. Albastră, Cluj, 2009, p.144)

b) The passive subject of the crime is the natural or legal (public or private) person whose patrimony was affected by the committing of the computer fraud.

The constitutive content of the criminal offence

A. The objective content

Information and communication technologies offer a lot of possibilities to commit computer frauds; they also facilitate the committing of these offences by the possibility to act from a great distance or the misuse of authorizations granted, by the low cost of committing these crimes and the low risk to which the perpetrators are exposed[7].

The material element consists in the action of inputting, modifying or deleting computer data, by restricting access to computer data, or by hindering in any way the operation of a computer system.

Data input refers to the introduction of inaccurate data or the introduction without an authorization of computer data, with reference to data that did not previously exist in the respective system.

Data modification includes the alteration, variations or partial changes of computer data, resulting in the emergence of new computer data that are different from the original ones and inconsistent with reality.

For example, such a mode of action is data manipulation. Data manipulation refers to the process by which a person changes the data in a computer as a means to cause damages to the owner of that computer – damages that are not physical in nature, but which almost always have financial consequences.

A possible situation for this type of action could be that of former employees who use the security codes to gain access to bank records and then transfer the money into a bank account where the money cannot be detected. The rounding-down or salami technique (as it is sometimes referred to, given its "slicing"effect) is an example of data manipulation involving financial information. Instructions regarding the software program are secretly inserted in the network or the computer and when there are changes in the bank accounts, the program will round down the deposits and transfer the excess funds to a separate account. Once the account has reached a certain level, the money will be transferred into a separate account[8].

Data deletion refers to the erasure of data from physical devices, which are no longer available for licit electronic transactions, or may also be equivalent to the destruction of the data carrier.

Access restriction includes withholding, hiding, encrypting or changing the authorizations of legitimate users.

The changing of the authorizations of legitimate users, for example, can be achieved by learning their passwords and changing them by using a keylogger. The keylogging process takes place by means of software programs that can be installed on the user's computer without their knowledge, but also through hardware means, i.e. physical equipment, which are not only impossible to detect by the antivirus software, but for the average user it is very difficult even to visually spot them.

Once installed, the keylogger will automatically start recording every pressing of the button on the keyboard, so with the help of it one can find out what was said when using Messenger, what websites were visited, but also the user's passwords.

---

[7] George Antoniu, Constantin Duvac, Daniela Iuliana Lămășanu, Ilie Pascu, Constantin Sima, Tudorel Toader, Ioana Vasiu*, Explicațiile preliminare ale noului Cod penal, Vol. III (Articolele 188-256)-Partea specială,* Ed. Universul Juridic, București, 2013, p. 601 (*Preliminary Explanations of the New Criminal Code*, *Vol. III (Articles 188-256) - The Special Part*, Universul Juridic Publishing House, Bucharest, 2013, p. 601)

[8] R. Moore, op.cit., p.37

The hindrance of the operation of a computer system includes physical attacks (such as wire-cutting or power supply interruption) and logical attacks, which prevent the computer's normal startup of (for example, by changing the initial settings), denial-of-service attacks (which aim at blocking access to a system or service offered by the computer through depletion of a resource allocated to the respective system or service – for example, the bandwidth or the number of simultaneous clients that can be answered), as well as system crash, by resorting to computer viruses.

Computer viruses are actually programs that infect a computer's executable files. Any program that replicates without the user's consent is a virus. Once the virus has infected a computer its first task is to multiply itself by spreading to other computer systems.

The damage caused by a virus is called payload (viral load). The trigger for viral action is the condition or the event that activates the virus, which can be a calendar date, the running of a program or sometimes even the connection to the Internet.

Another way of hindering the operation of the computer system is by using Trojan horses. A Trojan horse is a program that performs an apparently useful action, while in fact carrying out destructive actions that remain unknown to the user[9].

This program uses a method of instruction insertion into a program so that the program will perform an unauthorized function while executing a seemingly ordinary one[10].

The immediate consequence of these actions is that they produce a result, consisting in material prejudice for the aggrieved party, whereas the Criminal Code of the Republic of Moldova requires that at the time of committing the offence the damage value should exceed the equivalent of 50,000 MDL.

B. The subjective content

With this offence, guilt is only present as direct intention qualified by purpose. Thus, the perpetrator's action is carried out in order to obtain a material benefit for oneself or another. It is not necessary to actually achieve that benefit, the pursuit of it suffices[11].

Forms. Punishment

Preparatory acts, although possible and sometimes necessary are not criminalized, therefore are not punishable.

Attempt is possible and is punished (according to Art. 252 of the new Criminal Code).

The criminal offence is considered as completed when the perpetrator has introduced, modified or deleted in any way the data in a computer system or has restricted access to the respective data or has hindered in any way the operation of a computer system, thus causing a patrimonial loss to a person.

The offence can also be present in a serial form. It ends when the last act criminalized by the lawmaker has been achieved.

Penalties

In the new Criminal Code, the act of computer fraud is punishable with imprisonment from 2 to 7 years, a penalty which is lower than that provided by the old regulation, namely in Art. 49 of Law no. 161/2003, which was imprisonment from 3 to 12 years.

Under the Criminal Code of the Republic of Moldova computer fraud is punishable by a fine of 1,000 to 1,500 conventional units or by unpaid community work from 150 to 200 hours or by imprisonment from 2 to 5 years.

If the offence is committed by an organized criminal group or a criminal organization and it causes large-scale damages, the punishment will be imprisonment from 4 to 9 years.

---

[9] Debra Littlejohn Shinde*, Scene of the Cybercrime. Computer Forensics Handbook*, Syngress Publishing, Rockland Massachusetts, 2002, p.326

[10] Adrian Cristian Moise, *Metodologia investigării criminalistice a infracțiunilor informatice*, Ed. Universul Juridic, București, 2011, p. 145 (*Methodology of Cybercrime Forensic Investigation,* Universul Juridic Publishing House, Bucharest, 2011, p. 145)

[11] V. Dobrinoiu and collaborators, op. cit., p.334

Conclusions

Cyber criminals elude the physical limitations that govern real-world crimes, because the physical proximity of the perpetrator and the victim is not necessary. All that a cybercriminal needs is a computer connected to the Internet.

The apparent anonymity that users are enjoying when browsing the Internet leaves place for vulnerability to improper, immoral and illegal usage.

References

1. George Antoniu, Constantin Duvac, Daniela Iuliana Lămășanu, Ilie Pascu, Constantin Sima, Tudorel Toader, Ioana Vasiu*, Explicațiile preliminare ale noului Cod penal, Vol. III (Articolele 188-256) - Partea specială,* Ed. Universul Juridic, București, 2013 (*Preliminary Explanations of the New Criminal Code*, *Vol. III (Articles 188-256) – The Special Part*, Universul Juridic Publishing House, Bucharest, 2013)
2. Vasile Dobrinoiu, Mihai Adrian, Mirela Gorunescu, Maxim Dobrinoiu, Ilie Pascu, Ioan Chiş, *Noul Cod penal comentat*, Volumul II-Partea specială, Ed. Universul Juridic, București, 2012 (*The New Criminal Code Commented*, Volume II – The Special Part, Universul Juridic Publishing House, Bucharest, 2012)
3. Adrian Cristian Moise, *Metodologia investigării criminalistice a infracțiunilor informatice*, Ed. Universul Juridic, București, 2011 (*Methodology of Cybercrime Forensic Investigation,* Universul Juridic Publishing House, Bucharest, 2011)
4. Alexandru Boroi, *Drept penal. Parte specială, Conform noului Cod penal*, Ed. C.H.Beck, București, 2011 (*Criminal Law. Special Part, According to the New Criminal Code*, C.H.Beck Publishing House, Bucharest, 2011)
5. Chuck Easttom and Det. Jeff Taylor, *Computer Crime, Investigation and the Law*, Course Technology, a part of Cengage Learning PTR, Boston, 2011
6. Robert Moore*, Investigating high-technology computer crime, second edition*, Elsevier, 2010
7. Ioana Vasiu, Lucian Vasiu, *Informatică juridică și drept informatic*, Ed. Albastră, Cluj, 2009 (*Legal Information Technology and Information Technology Law,* Publishing House: Ed. Albastră, Cluj, 2009)
8. Alexei Barbăneagră, Gheorghe Alecu, Viorel Berliba, Vitalie Budeci, Trofim Carpov, Valeriu Cușnir, Radion Cojocaru, Alexandru Mariț, Tudor Popovici, Gheorghe Ulianovschi, Xenofon Ulianovschi, Nicolae Ursu, Victor Volcinschi, *Codul penal al Republicii Moldova: Comentariu*, Tipografia Reclama, Chișinău, 2009 (*Criminal Code of the Republic of Moldova: Commentary*, Reclama Printing House, Chisinau, 2009)
9. Debra Littlejohn Shinde*, Scene of the Cybercrime. Computer Forensics Handbook*, Syngress Publishing, Rockland Massachusetts, 2002