THE CYBERCRIME CHALLENGE: DOES THE ROMANIAN LEGISLATION ANSWER ADEQUATELY?

Ph.D. Ioana Vasiu*
Faculty of Law, Babeș-Bolyai University, Cluj-Napoca, Romania

PhD MBA Lucian Vasiu**
Faculty of Law, Babeș-Bolyai University, Cluj-Napoca, Romania

Abstract
Several factors combine to create many criminal opportunities in cyberspace, posing a growing challenge to stakeholders. In the fight against cybercrimes, legal measures play an essential role. Considering the evolving threats, there is a clear need to constantly update and harmonize the legal provisions. In this article, we discuss the cybersecurity attributes, the categories of cybercrime, present an overview of Romanian cybercrime legislation with respect to the most significant or prevalent offenses and assess its adequacy in the current context. We conclude with recommendations.

Keywords: cybercrime, threat, security attributes, vulnerability, Romanian criminal law.

1. Introduction
Along with many socio-economic benefits, information and communication technologies brought about many challenges. In particular, the attacks against information systems are globally considered very concerning¹. Whether

The cybercrime challenge: does the Romanian legislation answer adequately?

perpetrated from outside or inside, the potential economic, operational or reputational consequences of successful computer attacks can be very significant, at individual, organizational and even national or international level. Consequently, as the European Commission emphasizes, the fight against cybercrimes should be a core element in the overall strategy that aims to protect the security of information systems.

Cybercrimes now represent an important percentage of all crimes. This increase in cybercrimes is the result of the unprecedented opportunities that cyberspace and the global economy present to perpetrators, whether small-scale criminals or highly organized crime syndicates. These criminal opportunities arise foremost from the very large number of software vulnerabilities (some allowing zero-day attacks) and evolving threats. Of particular concern are botnets,

---


3 The threat posed by insiders is very real and is discussed in numerous publications. See Adam Cummings et al., Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector (2012); Verizon, 2012 Data breach investigations report, Study conducted by the Verizon RISK Team with cooperation from United States Secret Service et al. (2012); Frank L. Greitzer et al., Combating the Insider Cyber Threat, IEEE SECURITY & PRIVACY, January/February, 6(1), 61-64 (2008).


7 Vulnerability can be defined as a coding error that allows a perpetrator to execute commands as a legitimate or authorized user, to access computer data contrary to the access restrictions in place, or to conduct a denial of service attack.


10 Botnets are sets of computers controlled remotely by the perpetrator(s) and used in large-scale attacks against other computer systems. See details in Rafael A. Rodriguez-Gómez, Gabriel Maciá-Fernández & Pedro García-Teodoro, Survey and taxonomy of botnet research through life-cycle, ACM COMPUTING SURVEYS, 45(4), 45 (2013).
phishing techniques\textsuperscript{11}, and computer contaminants, also known as malware\textsuperscript{12}, particularly considering the availability of advanced tools and services on the black market as commodities\textsuperscript{13}. Further, considering that cybercrime proceeds make it more profitable than the combined global trade in marijuana, cocaine and heroin\textsuperscript{14}, and the constant development of new criminal tools and approaches, which makes these crimes increasingly sophisticated\textsuperscript{15}, we can only expect a rise in cybercrime prevalence in the future.

The fight against cybercrimes can only be successful if approached holistically. According to an ITU publication\textsuperscript{16}, such an approach should be based on five pillars: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, and International Cooperation. In Romania, as stated in Government Ordinance No. 1040/2010, the prevention and combating of cybercrimes is a strategic objective. The importance of fighting cybercriminality is further emphasized in the Government Decision No. 271/2013 for approving the Romanian cybersecurity strategy and national action plan on the implementation of the national cybersecurity system\textsuperscript{17}. Both documents acknowledge the importance played by the legal measures in the fight against cybercrimes and underline the need to update, improve and harmonize the legislation.

This article aims to present an overview of the Romanian cybercrime legislation with respect to the most serious or prevalent offenses and to assess its readiness or adequacy in the current threats context. The remaining of this article is structured as follows: Part I explains the security attributes associated with computer data and systems; Part II looks into categories of cybercrime; Part III presents Romanian criminal law provisions. Finally, we draw our conclusion.

\textsuperscript{11} Attacks that aim to acquire passwords or personal information, typically carried out via e-mails or comments on social networking service that contain malicious links to phony websites or embedded code in attachments.


\textsuperscript{13} See, e.g., Thomas J. Holt, Examining the Forces Shaping Cybercrime Markets Online, SOCIAL SCIENCE COMPUTER REVIEW, 31 (2), 165-177 (2013).


\textsuperscript{16} Marko Gercke, Understanding Cybercrime: A guide for developing countries (2011).

\textsuperscript{17} Published in Monitorul Oficial, Part I, No. 296, 23.05.2013.
2. Cybersecurity attributes

To accomplish their goals, criminals breach one or more security attributes associated with the proper use of computer data and systems. The most widely discussed security attributes by researchers and commentators are confidentiality, integrity and availability.

Confidentiality is an attribute that concerns computer data that should not be obtained or read without right. Confidentiality is very important when disclosures would significantly harm the victim, for instance the case of trade secrets or personal information (such as medical records, financial records or attorney-client communications). Confidentiality can have several levels of restriction, from restrictions to reading, printing or transmitting data through a computer system, to restrictions regarding even the existence of certain data.

Integrity refers to maintaining accurate and complete data unaltered in an improper or subversive manner. Data integrity concerns data stored, processed or in transit. In the context of databases, data integrity also regards the metadata and the functions used.

Availability refers to computer data and systems timely and reliably obtainable or accessible for legitimate users at all times or upon demand, as per their authorized use. Availability implies preventing all actions that negatively or improperly affect authorized access to or use of data or systems, including actions that encrypt, delete, delay or deny access to data or services.

Parker proposes three more security attributes: Authenticity (that is, assurance that a message, transaction or communication is from the source it claims to be from), Possession or Control (in certain situations, computer data could be possessed or controlled by unauthorized persons without breaching the confidentiality attribute) and Utility (which concerns the usefulness of computer data). An important study discusses these six attributes in paired format: Confidentiality&Possession, Integrity & Authenticity, and Availability & Utility.

To these attributes, we would add Legitimate use, which refers to use of computer data or systems in compliance with all applicable local, state, federal and foreign laws, as well as system owner’s policies.

3. Categories of cybercrime

There is no widely agreed definition of what constitutes cybercrime; moreover, terms like ‘computer crime’, ‘cybercrime’, ‘e-crime’, ‘network crime’, ‘Internet crime’, ‘computer-related crime’ or ‘hi(gh)-tech(nology) crime’ are used interchangeably in various publications. Professor Brenner identifies a range of

---

19 See Verizon, supra note 3 at 5-6.
cybercrimes, including crimes that target computers (such as the use of computer contaminants or distributed denial of service attacks) and crimes in which the computer is used as a tool (such as cyber extortion or theft). The Convention on Cybercrime\textsuperscript{21} proposes four categories of cybercrime: Offenses against the confidentiality, integrity and availability of computer data and systems (e.g., illegal access or system interference), Computer-related offenses (e.g., computer-related fraud), Content-related offenses (e.g., offenses related to child pornography), and Offenses related to infringements of copyright and related rights. Gercke\textsuperscript{22} uses the classification proposed in the Convention on Cybercrime, although he acknowledges overlaps due to typology not being “wholly consistent, as it is not based on a sole criterion to differentiate between categories”.

COM(2007) 267 final\textsuperscript{23} proposes three categories of cybercrimes: traditional forms of crime (such as fraud), dissemination of illegal content over electronic media (such as child pornography), and crimes unique to electronic networks (such as denial of service attacks). The United Nations Office on Drugs and Crime (UNODC)\textsuperscript{24} classification of cybercrimes comprises three broad categories that include acts widely regarded as cybercrime: Acts against the confidentiality, integrity and availability of computer data or systems, Computer-related acts for personal or financial gain or harm, Computer content-related acts, and one category named Other cybercrime acts, which includes acts that may also be considered cybercrimes.

4. Romanian cybercrime legal provisions
In this Part, we discuss the Romanian legal provisions with respect to main misconduct against the confidentiality, integrity or availability of computer data or systems, acts for illegal personal or financial gain, and acts involving illegal content. The limitations of this article leaves outside discussion other offenses, not least important, such as intellectual property infringements, hate speech or grooming.

A. Illegal access, exploitation and interference
Criminal law provisions must protect computer data and systems from unauthorized exploitation and subversion (such as disrupting, disabling or maliciously controlling computer systems), which actually translate into protection against actions that would breach the security attributes discussed above.

Law No. 161/2003 contains, in Chapter II of Title III, provisions regarding the prevention of cybercrimes, including prevention programs, promotion of policies, procedures and standards, realization of studies that examine the causes and

\textsuperscript{22} Gercke, \textit{supra} note 16 at 29-30.
conditions that drive cybercrimes, the maintenance of a database dedicated to cybercrimes, and the organization of education and training programs. Title III’s Chapter III of Law No. 161/2003 follows very closely the Convention on Cybercrime and, in Section 1 (Art. 42-47), incriminates offenses against the confidentiality and integrity of computer data and systems. While an important example of legal measures at global level, we would remark that the Convention needs significant updates, in order to adequately address the important developments that occurred since its drafting.

Art. 42 of Law No. 161/2003 prohibits the access without right to computer systems. According to this provision, a person acts ‘without right’ if it is not authorized by law or by a valid contract, exceeds the limits of authorization or does not have the permission from the entitled entity (that is, system owner or administrator) to use the computer system (Art. 35). The Explanatory Report for the Convention on Cybercrime defines access as comprising “the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data)”. We would define access to a computer system as the ability to successfully read, write or execute computer files. Points (2) and (3) of Art. 42 stipulate more severe penalties for situations when access to a computer system without right is made in the attempt to obtain computer data or by breaching security measures in place. Art. 43 makes it illegal to intercept, without right, non-public computer data sent to or transmitted from or within a computer system. This provision aims to protect the right of privacy and the confidentiality of data sent from or via computer systems.

Criminalization of computer damage or interference can be found in two separate provisions. Art. 44 makes it illegal to modify, delete or alter computer data, to restrict access to computer data and to transfer without authorization data from a computer system or storage device without right. Art. 45 criminalizes the impairment, without right, of a computer system by the input, transmission, modification, deletion or altering of computer data or by restricting access to such data. This provision stipulates that the impairment of the proper functioning of computer systems must be ‘serious’ to cause criminal sanction, but does not attempt to define this broad term or concept. Further, there are no provision for the more serious attacks against systems that are part of critical infrastructure.

Art. 46 concerns access devices and criminalizes the possession, making, selling, importation, distribution or providing, without right, of devices or computer programs that would be used to perpetrate the offenses criminalized in Art. 42-45; it also makes it illegal to possess, make, sell, import, distribute or provide, without right, passwords, access codes or computer data that would allow access to a computer system to perpetrate the offenses criminalized in Art. 42-45. Art. 47 stipulates that the attempts to perpetrate any of the offenses address in Art. 42-46 shall be punished.
Section 2 of Law No. 161/2003 comprises computer-related crimes. Art. 48 criminalizes an offense that is the high-tech variant of physical forgery of documents, to protect the legal interest in the integrity and reliability of computer data, as this has consequences for legal relations. As the Explanatory Report for the Convention on Cybercrime emphasizes, “computer-related forgery involves unauthorized creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception”. Art. 49 criminalizes computer-related fraud, which is understood to mean the causing of patrimonial loss by any unauthorized computer data input, altering or deletion, the restriction of access to computer data or by the impairment of the normal functioning of a computer system, with the intent to obtain a material benefit for themselves or others.

The new Romanian Penal Code (Law No. 286/2009) also contains provisions that regard the security of computer data and systems. Chapter VI of Title VII (Crimes against public safety) criminalizes, in Art. 360-366, the following offenses: illegal access to a computer system, illegal interception of a computer data transmission, altering of computer data, impairment of computer systems, unauthorized transfer of computer data, and attempts to perpetrate these offenses, respectively. These articles have very similar provisions to those found in Law No. 161/2003, the only significant difference being a lower punishment for these offenses. Art. 325, part of Title VI (Chapter III), criminalizes computer forgery (identical with Art. 48 of Law No. 161/2003, except for the lower punishment). Art. 391(3), part of Title IX (Electoral crimes), prohibits the use of computer programs that would alter the recording or computation or voting results, while Art. 391(4) prohibits computer data or procedures input that would alter the election result.

In Chapter IV of Title II (Art. 250-252), the new Romanian Penal Code criminalizes frauds perpetrated using computer systems or electronic payment instruments. Art. 249, very similar to Art. 49 of Law No. 161/2003, criminalizes computer fraud. Art. 250 makes it illegal to use, without authorization, electronic payment instruments or data that identify such instruments, the unauthorized use of identification data or the use of false identification data, and the transmission of identification data to third parties to fraudulently use such data. Art. 251 addresses the acceptance of fraudulent financial transactions knowing that the electronic payment instrument is counterfeited or used without the owner’s consent. Art. 252 stipulates that attempts to perpetrate these offenses are punished. Provisions regarding crimes related to the issuing and use of electronic payment instruments and the use of identification data can also be found in Law No. 365/2002, Chapter VIII (Art. 24-28).
B. Illegal content

The digital environment has enormously increased the possibilities to perpetrate content-related offenses. Predominant among these offenses is the creation, access, and distribution of child pornography. In the United States, for instance, child pornography, as observed in one case, is one of the fastest growing areas of prosecution by the U.S. Justice Department\(^{25}\). Sexual exploitation of children is a very serious form of violence against them. Further, as observed in *United States v. C.R.*\(^{26}\), “many children who are not physically injured in the making of child pornography grow up knowing, or learning later, that their abuse has been frozen in time—sold, circulated, and traded long after physical trauma ended”. At international level, the main instrument in the protection of children, including against sexual exploitation, is the United Nations Convention on the Rights of the Child (UNCRC), adopted in 1989. In 2011, United Nations Resolution 2011/33 further stressed the need to effectively combat the sexual exploitation of children in the digital age\(^{27}\).

Romanian criminal provision regarding child pornography can be found in Section III of Law No. 161/2003. Art. 51 prohibits the production for distribution, offering or providing, disseminating or transmitting, procuring for himself or for another of such materials through information systems, as well as the possession of such materials in an information system or data storage system. The new Penal Code defines ‘child pornography’ as any material depicting a minor engaged in explicit sexual behaviour or material that, although does not present a person, simulates, in a credible way, a minor engaged in such behaviour, and criminalizes, in Art. 374, the production, possession for display or distribution, purchase, storage, display, promotion, distribution and provision in every way of child pornography materials. Access to such materials, through information systems or other electronic communication means, is also criminalized.

Cyberstalking is a special form of stalking that involves the use of information and communication technologies as the medium and the means of harassment or intimidation\(^{28}\). Cyberstalking is a violation of fundamental human rights, such as the right to life, liberty and security, and can amount to serious interference with the victim’s privacy, family or correspondence. Cyberstalking is very prevalent nowadays and can have dramatic consequences for victims, especially in cases


where the perpetrator is obsessed or deranged. The new Penal Code, in Art. 208 (2), incriminates phone calls or distance communications which, by frequency or content, causes fear to a person.

5. Conclusion

Cybercrimes encompass a broad range of acts or conducts and can result in significant adverse effects. Consequently, the prevention and combating of cybercrimes must be paramount to stakeholders. Adequate legislation is fundamental in the overall effort to answering the cybercrime challenge.

In this article, we discussed the Romanian criminal law framework with respect to the most serious or prevalent cybercrimes. The Romanian legal framework is based on the Convention on Cybercrime, which no longer provides an appropriate response to current cyberthreats. Further, the Romanian legal provisions are often vague and dispersed in a confusing way. Consequently, we believe that the effectiveness of existing legal measures needs to be reconsidered.

There is a need to better describe, in an unambiguous manner, the elements of the prohibited conduct and take into account the recent years developments in computer technology and perpetration techniques. We argue that there is a clear need to update the legal framework according to the new shapes of cybercrime. In particular, taking into account the very serious threat posed by malicious software, we consider that the production, possession, use or traffic of such programs must be penalized as a very serious offense. We also consider that there should be criminal penalties for carrying out phishing attacks, for false online personation and for the creation and exploitation of botnets. Further, cybercrimes and sentencing must be correlated: as an important deterrent, punishment needs to be more severe, not softened, as the new Penal Code does. Finally, we believe that laws must better address cybersecurity, investigation and evidence collection issues, aspects regarding jurisdiction and international cooperation, and the development of programs regarding awareness raising, education and training of employees.

References:


