International Journal of Multidisciplinary Research and Development
Online ISSN: 2349-4182, Print ISSN: 2349-5979; Impact Factor: RJIF 5.72
Received: 15-11-2019; Accepted: 16-12-2019
www.allsubjectjournal.com
Volume 7; Issue 1; January 2020; Page No. 190-191

Cybercrime, the challenge of modern times

Dorina Saja
University of Tirana, Faculty of Law, Department of Criminal Law, Albania

Abstract
The process of solving a problem consists of a detailed recognition of it. This work aims to deeply recognize the cybercrime phenomenon, because through recognition we can achieve sustainable theories to the phenomenon and create plain legal norms.
The existing theories on cybercrime are still in their initial phase that is why I focused on brand new theories that would explain the phenomenon.
Also, I tried to explain the key factors that the perpetrators of the law face during the investigation and assignment of the right legal definitions of the phenomenon. Framing a profile about cybercrime that would help the police in their work process and different researchers, is of a great importance. Even though framing a comprehensive profiling method seems to require a hard work. Not just because we are dealing with a new phenomenon, but it is constantly developing.
I hope this helps you clarify your point of view on cybercrime.

Keywords: cybercrime, computer incidents, the convent of cybercrime, computer emergency

1. Introduction
Life in the 21st century is strongly related to technology and the society is always getting closer and closer to it. Despite the facilities that the usage of computers and gadgets bring to the daily life, we have to emphasize the fact that not only do they facilitate the daily life, but also the criminal activities of different individuals. In many cases the computers are used as a tool to commit penal acts, as their goals.
Above all, in my opinion, the most important detail is the recognition of the phenomenon because through recognition we can achieve a convenient solution to the problem, beginning with a specific law definition and assignment of clear and comprehensive legal norms. Cyber criminology is a fast developing phenomenon and being a new topic in the criminal law, writings about it will never be enough to effectively face the problem.

2. The Definition
Despite the fact that it is fast developing and becoming closer to reality, it is difficult to define it with a unique and specific term. Cybercrime is the crime that involves a computer or a Network. The computer may have been used in committing the crime, or may be the target. Cybercrime can be defined as: "Offences that are committed against individuals or a group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (chat rooms, emails) and mobile phones (Bluetooth/SMS/MMS). Cybercrime may threaten a person or a nation's security and financial health. The problem caused by those kinds of crime are of a great concern, especially hacking, copyright, child pornography. There are many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed, lawfully or not.

3. Typology of Cybercrime
Even though the typologies seem to be similar in the aspect of the type of acts, many researchers use different methods to deliver the research. The term itself "cybercrime" is used in a wide variety of criminal acts. It is actually difficult to develop a typology or a system of classification on cybercrime because the actual crimes include a wide variety of violations. We can develop a kind of approach based on The Convent of Cybercrime [1], divided into 4 different types of violations [2]:

a. Violation against cofidelity, integrity and disponobility of computer data and systems [3];
b. Violation related to the computer [4];
c. Violation related to the content [5] and
d. Violation related to the authorized copyright [6]

[1] Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. Regarding the Convention on Cybercrime see: Sofaer, Toëard an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; Gercke, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 et seq.; Gercke, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et seq.; Aldesco, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime.
[2] The same typology is used by the ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008. The report is available at: ëëë.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
[3] Art. 2 (Illegal access), Art. 3 (Illegal interception), Art. 4 (Data interference), Art. 5 (System interference), Art. 6 (Misuse of devices). For more information about the offences, see below: § 6.2.
[4] Neni 7 (Computer-related forgery), Art. 8 (Computer-related fraud). For more information about the offences, see below: § 6.2.
[5] Art. 9 (Offences related to child pornography). For more information about the offences, see below: § 6.2.
[6] Art. 10 (Offences related to infringements of copyright and related rights). For more information about the offences, see below: § 6.2.

This kind of typology is not thoroughly sustainable because it is not based on a single criteria to make the differentiation between categories.

4. Key Factors

A considerable part of the general communication depends on TIK and internet based services including VoIP calls or email communications. TIK is responsible for supervision and management functions in buildings, vehicles and aviation services. Energy, and water supply, also communication services depend on TIK. The integrity of TIK in everyday life is likely to be continued. Being supported by TIK makes systems and services more vulnerable against crimes of critical infrastructure. Short cuts in services may cause huge financial harm to e commerce business. Not only civil communication can be interrupted by offences, but also military services can be threatened because of supporting TIK. The existing technical infrastructure has got some deficiencies for instance: monoculture and homogeneity of the operating systems. Many private operating systems and SME use the Microsoft operating system making it easier for the violators as a target.

5. Legal Challenges

The basis of investigating the cybercrime is the right legislation. Even though legislators should pay a continuous attention to the internet development and monitor to the affectivity of legal provisions, especially controlling the speed of network technological development. Historically new computer systems or internet related technologies have always caused the commission of new types of crimes, just after they appeared. A well-known example is the development of computer networks in the 1970s, the first unauthorized approach in computer networks happened later. Similarly the first violations of Software took place after the usage of private computers in 1980, when the systems were used to copy the program's products. The violation cannot be followed legally without the integration of cybercrime acts. The development of computer emergency team (CERT) [7], computer incidents team, reaction to computer security incidents team and other facilities have really improved the situation. The identification of the deficiencies in the penal code to make effective legal basis is important to compare the status of penal legal provisions in the national law regarding the requirements of different kinds of penal acts. In many cases the existing laws can respond to new varieties of existing crimes (laws for falsification can be easily applied to electronic documents.

The formulation of cybercrime legislation can result in considerable dublifications and resource loss. Also it is necessary to monitor the development of international strategies and standards. Without the international harmonization of the penal national legal provisions, the war against transnational computer crime will face serious difficulties because of national incompatible legislation. That is why the international efforts in the harmonization of different national penal laws are always getting important. National Law can benefit experiences of other countries and international professional law advice.

6. Conclusion

Cybercrime is actually a widespread phenomenon. In fact media mentions more those types of cybercrime all over the world. Even though there is enough space for the literature to be improved, because existing theories do not include a general explanation of the phenomenon. Sometimes the interpretations are really alike. Even though the development of different theories on cybercrime help the research work of law enforcement in finding the solution. The analysis of the factors that contribute the further development of cybercrime helps in the formulation of strategies and penal politics related to the prevention of cybercrime and even more, the treatment of criminals aiming the real punishment: rehabilitation. During the analysis of the key factors of cybercrime we can discover the types of cybercrimes and the reason of the spreading into different areas. The recognition of the key factors that cause cybercrime is the most important element in finding the most convenient solution to the problem

7. References

1. Carter, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin.
2. Cornish, Derek & Clarke, Ronald V. "Introduction" in the Reasoning Criminal, 1986.
3. Crozier B. A Theory of Conflict. Hamish Macmillan, London, 1974.
4. Garcia-Murillo. Regulatory responses to convergence: experiences from four countries, Info, 2005, 7.
5. Jaishankar K. Cyber criminology: Evolving a novel discipline with a new journal. International Journal of Cyber Criminology, 2007.
6. Jaishankar K. Space transition theory of cybercrimes, 2008.
7. Mann D, Sutton M. NetCrime. More change in the organisation of thieving. British Journal of Criminology, 1999.
8. Michael Bachmann. The Risk Propensity and Rationality of Computer Hackers.
9. Mira Carignan. L'origine Géographique En Tant Que Facteur Explicatif De La Cyberdélinquance, 2015.
10. Moon B, McCluskey J, et McCluskey CP. A general theory of crime and computer crime: An empirical Test. Journal of Criminal Justice, 2010.
11. Nhan J, Bachmann M. Developments in cyber criminology, 2010.
12. Roger MK. A two-dimensional circumplez approach to the development of a hacker taxonomy. Digital investigation, 2006.
13. Wall DS. Crime and the internet. Routledge, 2003.
14. Yar M. Computer hacking: just another case of juvenile delinquency? The Howard journal, 2005.
15. Zimmer E, Hunter D. 'Risk and the Internet: Perception and Reality', 1999.

[7] Computer Emergency Response Team. U themelua në 1988 pas incidentit me "Morris Worm" që solli ndalimin e 10 përqind të sistemeve të Internetit në nëntor të 1988.