CYBER-CRIMINOLOGY – A NEW FIELD OF SCIENTIFIC RESEARCH AND CRIMINOLOGICAL INVESTIGATION

Associate Professor Adrian Cristian MOISE, PhD.
Spiru Haret University of Bucharest, Romania
adriancristian.moise.@gmail.com

Abstract:
Virtual reality and the computer systems used in communications represent a challenge for traditional research in criminology, introducing new forms of deviant behaviour, crime and social control. Thus, a new notion and a new field of scientific research has emerged, called Cyber Criminology, which is defined as the study of the causality of crimes committed in cyberspace, a virtual space and their impact on physical space.The article aims to highlight the role of this new discipline Cyber-Criminology in criminological investigation and scientific research, which has the potential to become an independent discipline in academia and academia due to the dynamic expansion of its interdisciplinary content in teaching and research.
Keywords: *cyberspace, cybercrime, criminology, cyber-criminology, investigation.*

1. Introduction

The information society operates in a space called cyberspace which "represents a global domain in the information environment consisting of the interdependent network of information infrastructures, including the Internet, electronic communications networks, computer systems, processors and embedded controllers" [1].

A criminal activity also appeared in cyberspace.

The main advantages of the Internet, as well as its vulnerabilities have created a favorable framework for criminal activities, leading to the emergence of a new form of crime, cybercrime. Cybercrime has become a global problem that affects all countries in the world. Cybercrime is a broad and generic term that refers to crimes committed using computers and the Internet.

Criminology, which is a science with its own individuality, intended to study the causes, state and dynamics of the criminal phenomenon, the criminal, in order to improve the act of justice, the policy of social defence against crime and its prevention, can also be seen as a dimension of cyberspace crime. Criminology is the social science

that addresses the systems of criminal law, criminal procedural law and criminal enforcement law, as well as the relationship between criminal victim and state, being considered a descriptive science by creating specific theories based on the results of social life applied science by adopting measures and means to reduce crime, in close connection with other sciences: sociology, psychology, forensics, criminal law, criminal procedural law [2]. At the same time, Criminology is a scientific approach to study the social phenomenon of crime, in order to prevent and combat it [3].

Criminology as a theoretical-explanatory science, with implications of a practical, applied and in-depth examination, like the social sciences, aims at the system of research measures in the field, crime prevention and control, treatment of criminals, based on methods and techniques modern investigation [4].

Criminology is the social science that addresses the systems of criminal law, criminal procedural law and criminal enforcement law, as well as the relationship between criminal-victim-state, being a descriptive science by creating specific theories based on the results of social life, but also a science by adopting measures and means to reduce crime, in close connection with other sciences, such as criminal law, forensics, judicial psychology, legal sociology [5].

Since 1990, theoretical and practical research has observed how cyberspace has become a new field of criminal activity. Cyberspace has changed the nature and field of crime and victimization. Therefore, a new notion and discipline has emerged, called Cyber Criminology, defined by Indian criminologist Jaishankar Karupannan in the year 2007, “the study of the causality of crimes committed in cyberspace, a virtual space and their impact on physical space” [6].

Following the emergence of this new concept, Cyber Criminology, the following aspects have been highlighted in the literature: [7] firstly, the field of action of cybercrime should not be confused with the field of criminal investigation, but still it should have interferences with the field of forensic investigation of cybercrime; Secondly, the new university discipline Cyber Criminology must be an independent one in order to study the phenomenon of cybercrime from the point of view of the social sciences.

We consider that the discipline of Cyber Criminology has become in some legal systems, such as India and the United States of America, a discipline of university study and independent research, due to the dynamic expansion of its interdisciplinary content in the teaching and research process.

As this new discipline has become an independent one, we believe that it will have to face challenges related to the problems of teaching, research and professionalization of the recent discipline.

2. Aspects of the causality of crimes committed in cyberspace

Criminologists seek to collect important data about crime and interpret it scientifically. By developing empirically verified statements or hypotheses and including them in theories of the causality of crimes, criminologists hope to identify the causes that determine the commission of crimes.

One of the important objectives in criminological research is the elaboration of valid and precise theories regarding the causality of crimes. A theory can be defined as an abstract statement that explains why certain things happen or do not happen. A valid theory must have the ability to predict future events or observations of the phenomenon studied and be validated or tested by experiment or other form of empirical observation.
To study cybercrime, we appreciate an empirical approach to it, which includes estimating the magnitude of cybercrime, analyzing theories about the causality of cybercrime crime and victimization, and developing models to explore the impact. criminal justice policies for preventing and combating cyberspace crime. A comprehensive study of this phenomenon requires a multidisciplinary approach: knowledge of computer and telecommunications networks; an understanding of computer systems and how they can be attacked; knowledge of cyberspace crime legislation; an analytical approach to investigate the impact of cyberspace crime on society and to assess the effectiveness of cyberspace crime prevention measures.

Although the criminological analysis of cyberspace crime is much more present lately in the studies of the specialized literature, nevertheless, the criminological literature has not researched in detail the quantitative or analytical problems related to cybercrime.

3. Space Transition Theory

Ever since Criminology observed the emergence of cyberspace as a new place for criminal activity, there has been a need to develop a new theory to explain the causes of crimes in cyberspace. Thus emerged a theory specific to cybercrime, the Space Transition Theory, which explains criminal behavior in cyberspace.

To analyze criminal behaviour in cyberspace, Indian criminologist Karupannan Jaishankar developed the Theory of Space Transition that explains the causality of crimes committed in cyberspace. This theory refers to the movement of people from one space to another space (from physical space to cyberspace). The theory supports the idea that people behave differently when moving from one space to another.

The basic principles of this theory are as follows: [8]

- Persons with repressed criminal behavior in physical space tend to commit the crime in cyberspace, who would not otherwise commit it in physical space because of their status and position;
- The flexibility and anonymity of identity and the lack of deterrents in cyberspace give criminals the opportunity to commit crimes in cyberspace;
- The criminal behavior of criminals in cyberspace is imported into physical space, which can also be exported from physical space into cyberspace;
- The actions of cybercriminals and the dynamic spatial - temporal nature of cyberspace offer the chance for cybercriminals not to be discovered by the judiciary;
- Criminals from different nation states can associate in cyberspace in order to commit a crime in physical space. The association of criminals in the physical space is suitable for committing crimes in cyberspace;
- People in a closed society are more likely to commit a crime in cyberspace than people in an open society [9];
- The conflict between the norms and values of physical space with the norms and values of cyberspace determines the commission of crimes in cyberspace.

We appreciate that it is necessary to conduct studies in the future to test this theory to see if it explains the criminal activity in cyberspace.

4. Theory of Technology Enabled Crime, Policing, and Security

Theory of Technology Enabled Crime, Policing, and Security explains to society why cybercrime has developed with the help of innovations in information and communication technology [10]. Moreover, the Theory of Technology Enabled Crime, Policing, and Security complements the existing theories on the causality of cybercrime and on the development of information and communication technology.

The innovative use of information and communication technology has led to the emergence of new types of crime. Initially, these new types of crimes due to their complexity were not understood by law enforcement agencies, as they could not explain how criminals used these technologies to commit certain illegal acts [11].

Once the new crimes were understood by law enforcement, lawmakers were able to change the legislative framework by criminalizing these new types of illegal behaviours [12].

5. Conclusions

We believe that the new subject Cyber Criminology should be introduced into the curriculum as a compulsory subject in law schools, given the importance of the science of criminology and the expansion of the phenomenon of cybercrime worldwide. As this new discipline has become an independent one, we believe that it will have to face challenges related to the problems of teaching, research and professionalization of the recent discipline.

At the same time, we believe that criminological studies should be continued worldwide, in order to explain the causality of crimes in cyberspace.

References:

[1] Vasiu, Ioana; Vasiu,Lucian (2011). Cybercrime, Bucharest: Universul Juridic, p. 21.
[2] Mitchell Miller, J. (2009). Criminology as Social Science: Paradigmatic Resiliency and Shift in the 21st Century, in Mitchell Miller, J. (ed.), 21st Century Criminology. A Reference Handbook, London: SAGE Publications Ltd., pp. 2-3.
[3] Sutherland, E.; Cressey D. (1960). Principles of criminology, sixth edition,
Chicago: Lippincott, p. 3.
[4] Chipăilă, Ioan (2009). General Criminology. Craiova: Sitech, p. 17.
[5] Tănăsescu, Iancu; Tănăsescu, Camil; Tănăsescu, Gabriel (2003). Criminology, Bucharest: ALL Beck, p. 193.
[6] Jaishankar, Karupannan (2010).The Future of Cyber Criminology: Challenges and Opportunities, in International Journal of Cyber Criminology, January-July 2010, July-December 2010, vol. 4 (1&2), p. 26.

[7] Jaishankar, Karupannan (2010). The Future of Cyber Criminology: Challenges and Opportunities, in International Journal of Cyber Criminology, January-July 2010, July-December 2010, vol. 4 (1&2), p. 26.
[8] Jaishankar, Karupannan (2007). Establishing a theory of cyber crimes, in International Journal of Cyber Criminology, vol. 1, issue 2, July, 2007, p. 7.
[9] Jaishankar, Karupannan (2008). Space Transition Theory of cyber crimes, in
Schmalleger, F.J.; Pittaro M. (eds.), Crimes of the Internet, Upper Saddle River, New Jersey: Prentice Hall, pp. 283-301.
[10] McQuade III, S.C. (2009). Encyclopedia of Cybercrime, Westport, Connecticut: Greenwood Publishing Group, Inc., pp. 181-182.
[11] McQuade III, S.C. (2006).Technology-enabled Crime, in Policing and Security, vol. XXXII, no. 1, pp. 32-42.
[12] Moise, Adrian Cristian (2020). The criminological dimension of cyberspace crime, Bucharest: C.H. Beck Publishing House, pp. 86-87.