

PREFACE

Cyberspace poses various malicious and criminal activities performed by different actors: amateurs, criminal and terrorist organisations, Hacktivists, and state actors. Those activities pose a threat danger and have far-reaching consequences to the individual, organisation, community, society and even the state, as well as for various sectors and industries.

The book analyses the theoretical and practical aspects of Cyber and computer crime. *Adriana Iuliana Stancu* examined the criminological aspects of computer crime. She examined the current criminological study on electronic computer and computer crimes in this regard in Romania and internationally. The trials and convictions in computer crimes in Romania, statistics, legislation, classification and definitions of cyber threat actors and offenders. The study analyses computer crimes both from the offender's and the victim's perspectives. First is examining the causes and motivations of committed computer crimes – Biological, Psychological and Sociological orientations. Then, the study shed light on the criminological aspects of the victim of a computer crime. Finally the study

Tal Pavel analysed the practice of cybercrime activities relating to a specific threat actor and location – a Palestinian cyber threat actor, allegedly operated by Hamas from Gaza, for more than a decade.

We are most often exposed to APT hacking groups and their activities, as these are cyber-attacks by countries known for their offensive cyber activities, including Russia, China, North Korea and Iran. However, there is little research on APT hacking groups active in the Palestinian territories and by governmental entities. In light of this, the importance of this research is in the spotlight directed towards this arena and players who are usually not eligible for research other than those of research companies in the field of information security and cyber.

Some terrorist organisations are active in the digital space throughout the life cycle of a physical terrorist act.

This study aims at analysing the cyber offensive activities made by local Palestinian groups known by several nicknames, which have been active in the Palestinian arena for several years against various elements, including Israel. This study examines the group's activities over the years, its technological capability, the developments that have taken place in it, the goals of its attacks, and the attempts to associate this activity with the active players in the Palestinian arena.

The study's conclusions refer to the number of actual local Palestinian cyber threat actors, the level of technological sophistication, and the targets of their cyber-attacks across the years.

1. CRIMINOLOGICAL ASPECTS REGARDING COMPUTER CRIME

As a new technology, information technology was created to contribute to the progress of human society through the optimal use of information in all areas of life. There is no field in which computers have not penetrated and acquired significant importance in the control and smooth running of social and economic activities, in the remote transmission of information, and in communication. In some activities, the computer replaces human work, and the human becomes dependent on the proper functioning of the computer. Industry, commerce, the economy as a whole, medical services, and public administration depend to an increasing extent on the good use of information systems. To a decisive extent, human life is related to computer use in terms of, for example, medical interventions or air traffic.

The technological development and widespread use of computer systems have brought undeniable benefits but equally exposed society to several risks related to the bad-faith use of the same systems. Practically, the degree of dependence of public institutions, legal and private entities, on a similar degree of vulnerability, computer networks, and exposure to the illicit use of the same means.

Computer use brings benefits but also gives rise to new and sophisticated illicit activities. The consequences of these facts are not only economical and patrimonial but, by increasing the importance of IT systems in everyday life, affect many social relationships, including those related to the right to life.

1. The electronic computer was and is a first-order criminogenic factor that makes available to criminal conduct both a new object (the

information contained and processed by computer systems) and a new tool (Riti dot-Gov, 2023).

2. Computer crime can be studied through the lens of criminal legal provisions (of substantive criminal law), through the lens of criminal procedural aspects or from the point of view of the elements of forensic tactics related to investigating these crimes. Indeed, an indispensable component of understanding this phenomenon represents the criminological elements of cybercrime.

The current criminological study aims at bringing to the fore both the aspects related to the criminal information system, its profile, the motivations of the criminal act, the justifications for the conduct, as well as the aspects related to the victim of the computer crime, typology, post-delictum conduct starting from the results of the research on the matter carried out at a national and international level.

One of the Romanian criminal law's fundamental principles is the legality of incrimination, a principle illustrated by the Latin adage *nullum crimen sine lege*. In order to highlight its primary effect of imposing the non-retroactivity of criminal law, some authors (Girgiu, 2000, p. 30) preferred more nuanced formulations such as *nullum crimen sine lege praevia*.

An essential effect of this principle is that behaviour, a conduct can only be considered criminal to the extent that, prior to it, the law was enacted to prohibit that conduct under the sanction of punishment expressly. Alternatively, in computer crime, the special incriminations in Romania are relatively recent. As a result, the computer criminal was brought to the attention of Romanian criminologists at a relatively recent date.

At the international level, especially in the United States, Japan and Australia, there is a rich judicial practice in the matter, and some criminological studies, also cited in this paper, have focused on the computer criminal and its victims.

The premise from which we have started in the analysis of computer crime from a criminological aspect is that Romania is known as a rich source of specialists in information technology, specialists of a specific value. Equally, our country stood out for an impressive number of IT criminals.

Romanian universities have generated and continue to generate numerous IT specialists, well-rated in Romania, but especially in Western Europe, the United States, Asia, and the East. Many young people are being lured to work for software companies abroad (Romania tackles rise in cyber-crime, 2023).

Apart from computer science graduates, an impressive number of young people (pupils and/or students) stand out for their unique skills in using computer networks. In addition, the explosive development of the use of computer networks in Romania after 1990 encouraged the specialization of young people in this field. However, it inevitably led to increased criminality related to these networks' use. Electronic computers thus became an attraction for those interested in development and those who saw the exploitation of modern technology as a way to gain undue benefits (Riti dot-Gov, 2023).

1.1. The computer criminal

1.1.1. Peculiarities of the criminological study in the field of computer crimes

Criminological research, regardless of its object, whether we are talking about basic or applied research, must always be based on a set of theoretical and factual data that must be taken critically (Nistoreanu & Păun, 1995, p. 71). Viewed as a set of crimes committed over some time in a specific geographic territory, crime is an essentially quantitative phenomenon (Gassin, 1990, p. 105).

Collecting this data necessary for criminological studies has proven to be a complex problem for researchers, a deterrent for most initiatives in this sense.




Traditionally, crime is measured through various types of statistics. Statistics in the field of computer crime experienced a relative development in the 70s and 80s (Sieber, 2023, p. 21) when the phenomenon of computer crime - in terms of the number and types of crimes - was relatively low, consisting mainly of fraud, sabotage and espionage.

The extraordinary development of forms of computer crime after the mid-80s, through the emergence of computer piracy, computer manipulation and hacking, made such general statistics no longer find their unity. They were being abandoned one by one in many countries.

XXI century statistics find their usefulness only to the extent that categories and types of crimes differentiate them and have broad coverage areas.

These statistics were and are elaborated by criminologists, judicial authorities or, more recently, by corporations in the field of computer security. It is certain, however, that only a minimal number of the data provided as computer attacks end up being instrumented by the judicial bodies (by identifying the criminals and holding them accountable).

Thus, in the theory and practice of criminology, the forms of crime are also investigated according to the degree of knowledge, discovery, registration, verification and judicial resolution (Oancea, 1994). In this way, criminality is studied on three levels:

-  real criminality;
-  legal criminality;
-  apparent criminality.