

## THEORETICAL-CRIMINAL CONFUSION ABOUT WHETHER CYBERCRIME IS PART OF THE CRIMINAL NETWORKS OF ORGANIZED CRIME

SANTILLÁN MOLINA ALBERTO LEONEL<sup>1</sup>, VINUEZA OCHOA NELLY VALERIA<sup>2</sup>, BENAVIDES SALAZAR CRISTIAN FERNANDO<sup>3</sup>, SANTILLÁN OJEDA SALVATORE JOEL<sup>4</sup>

Universidad Regional Autónoma de Los Andes Santo Domingo. Ecuador.

E-mail: us.albertosantillan@uniandes.edu.ec

ORCID: <https://orcid.org/0000-0001-8517-8980>

E-mail: ub.nellyvinueza@uniandes.edu.ec

ORCID: <https://orcid.org/0000-0002-1348-5620>

E-mail: us.cristianbenavides@uniandes.edu.ec

ORCID: <https://orcid.org/0000-0002-4326-2137>

E-mail: ds.salvatorejs23@uniandes.edu.ec

ORCID: <https://orcid.org/0000-0003-4621-2132>

### ABSTRACT

*Organized crime is a structured group that brings together several people in a hierarchical order to commit serious crimes, and obtain economic, material or other benefits, while cybercriminality carries out illicit activities in cyberspace, by attacking systems, computers, with the use of technological tools. Information and communication technologies have allowed the automation of illicit operations, allowing to confuse if these activities converge in a single objective between the two types of crime, or if one depends on the other, therefore, the research problem lies in the theoretical-criminal confusion, whether cybercrime is a part of organized crime, or has its own sustenance due to this new generation of cyber criminals, with the objective of establishing theoretically the difference between the new cyber criminal generation that executes illicit acts in cyberspace, and organized crime whose actions are materially observable in society. The research was of a qualitative nature that used the historical-logical and analytical-synthetic methods to analyze organized crime and cybercrime in its new paradigm; and content analysis as a technique, concluding that cybercrime is not a criminal network of organized crime, dependent on it, but rather a group of independent technological criminals who venture into another class of platform, such as cyberspace. , and that they would provide their illicit service in response to supply and demand.*

**KEYWORDS:** *Organized crime, cybercriminality, cybercrime, cyberspace.*

### INTRODUCTION

Organized crime today is a structured group in which several people meet in a hierarchical, financed and logistically directed manner, for the execution of one or more serious crimes, with the purpose of an economic, material or any other type of benefit.

In this sense, the United Nations Convention against Transnational Organized Crime defines an organized criminal group as a

"A structured group of three or more persons which exists for a period of time and acts in concert for the purpose of committing one or more serious crimes, or offences established in accordance with this Convention, with a view to obtaining, directly or indirectly, a financial or other material benefit. (Organizacion de las Naciones Unidas, 2004, pág. 1)

Generally, the structure of these criminal organizations have vertical or horizontal hierarchical levels where we can establish that there are chiefs, deputy chiefs, directors, middle managers and executors, who carry out the orders given from the high command of the organization or its middle managers by domination of the will in apparatuses of organized power. The fundamental axis of organized crime is to maximize the economic, political, cultural, religious or any other benefits established in this criminal structure.

This criminal organization has migrated from being territorial in which it carried out its illicit activities within a certain territory circumscribed to a region or a country, to a transnational structure with expansion of cross-border illicit business, which currently makes obsolete the requirement of



territoriality to be able to sanction persons within a given country, which allows in a clear way the interoperability related between criminal enterprises selling illicit services, such as money laundering or hired killers.

Organized crime establishes various businesses that are committed in multiple illegal acts instrumental and necessary for the development of the criminal enterprise, whose purpose is to protect and ensure the viability of the organization and the business internally or externally, as well as the use of violence exercised within the organization, corruption of public authorities on a small or large scale, money laundering, associated with the main behaviors aimed at reducing the risk of detection and ensuring the viability and projection of the criminal group." (Gimenez-Salinas Framis, 2011, pág. 3)

Globalization in this 21st century as well as the growth of all activities from the financial, economic, social, political, sports, etc., have allowed an expansion of human actions in aid of information and communication technologies, and thus expand knowledge on issues such as: communication, education and others of a social nature.

However, they have also allowed "illicit activities to cross national borders amplifying the profits of criminals, as well as the degree of impact and social damage of these activities, affecting the security of people and state structures. (Rodriguez-Barrigón, 2011, pág. 15)

These antisocial structures called organized crime, refer specifically to those criminal organizations with "special characteristics that differentiate it from conventional criminality, its purpose being to commit more homogeneous or heterogeneous criminal behaviors". (Sanchez, 2012, pág. 32)

The technological advances that have been developed since the middle of the 20th century and now in this 21st century in computer matters and that is reflected in the automation of the operations of different companies, businesses, States or any other activity that uses ICT, have created an opportunity for attackers to explore new techniques that improve those tools they use to be able to carry out attacks on automated information systems, framing their conduct in cybercrime.

Cybercrime is the set of illicit activities committed in cyberspace, which have as their object the elements of computer systems or any other legal good, provided that in their planning, development and execution, the use of technological tools is decisive. (BOE, 2019, pág. 43443)

Cybercrime today and its technological capacity to overcome those political or geographical barriers that are established according to the territoriality of the peoples, has allowed cybercrime to be an effective tool for the operation and automation of the operations carried out by these criminal organizations outside the law. thus maintaining the flow of money, such as orders to be fulfilled through the Deep Web, totally inaccessible to police or intelligence organizations that seek to identify and individualize the components of these criminal structures.

The use of information and communication technologies as a basic tool to operationalize or organize any kind of activity in a company or business, is not what should be observed when analyzing the actions of organized crime, but that this configuration of the system is programmed for the commission of infractions, such as hacking, espionage or computer sabotage, or any other classification established as cybercrime.

Cybercrime and its management of cyberspace circumvents geographical barriers that make it one of the greatest challenges for community authorities, because they must know the operation of each of the systems in order to determine how this kind of crime is executed, and thus explain to the authorities its consummation and how they fit into the specific criminal type detailed in the criminal law. and differentiate it from the automation of its administrative, organizational or logistics activities, what is done is to use ICT as a means of administration.

The reality is that in this XXI century organized crime uses cybercrime that uses ICT as a tool for its criminal activities, as well as through the acquisition of goods and services offered on the Deep Web, which is a community market where you can obtain any kind of offer of a criminal nature.

In view of the above, the professor of the University of Oxford, Jonathan Lusthaus, in his article published in the Cycle of conferences "Black Hat, USA 2018, entitled: Is the mafia taking over Cybercrime? whose translation is: Is the cybercrime mafia taking over? and that this article was adapted from the text of his authorship: "Industry of Anonymity; Inside the Business of Cybercrime",



published in Cambridge, Mass. & London; by the division of academic publications: Harvard University Press, in which it considers that:

"There is a new generation of criminals that is not necessarily directly related under the control of organized crime, but is a new company managed by new entrepreneurs who hire the services of technically qualified personnel in the knowledge of information and communication technologies, which allow illicit activities from a new field in a totally different world such as cybernetics." (Lusthaus, 2018, pág. 8)

Therefore, the research problem lies in the confusion existing from the criminal theoretical field, of whether cybercrime is a part of organized crime, or has its own sustenance due to this new generation of cyber criminals.

Therefore, the objective of this research is to establish in a theoretical way the difference that exists between the new cybernetic criminal generation that executes illicit acts technically in cyberspace, and organized crime whose actions are materially observable in society.

### METHODS

The research was qualitative in which the following methods were used:

Historical-logical, which allowed an explanation of how the structure of organized crime as well as cybercrime was constituted.

Analytical-synthetic that allowed an explanation of the various definitions of both organized crime and cybercrime in order to establish their theoretical difference.

The research technique used was the analysis of content and other documentation related to the topic investigated, which allowed reaching the final conclusions based on research work related to the topic.

### RESULTS

#### Elements of organized crime

The basic elements of an organized criminal structure is that there is a plurality of people, as well as a hierarchical presence that is composed of a vertical or horizontal assembly with a series of rules or codes of conduct that allows establishing immediate obedience to the ascending hierarchical order, since in this class of structured groups of power, There is no disobedience or rebels, which would imply the elimination of each of its components.

Another of the basic elements in organized crime is the tendency to self-preservation on the part of its members, the fulfillment of the order of the man behind, that is, of the person who is at the top of the chain of command, to the point that the executor must comply with it to avoid collateral damage to both their relatives and the people who matter to them. This is the reason why definitely in organized crime groups there is absolute obedience to whoever commands it, due to the economic benefits they obtain, and that serves as a measure of pressure for the fulfillment of the order of the mediated author.

Within the guidelines that can be observed to characterize and differentiate certain criminal structures in observance of the levels of violence and organization, "the existence of 2 dimensions is recognized in organized crime: organized armed groups and organized criminal groups", whose form of execution of criminal acts, have to do mainly with ideology, objectives, aims or beliefs they pursue, such as in Islamist States, which are armed groups based on the Koran and the 114 Suras or Revelations delivered by the archangel Saint Gabriel to Muhammad, who seek to pierce with the sword of Islam the heart of the infidels, so they carry out terrorist acts in defense of their faith; or criminal enterprises dedicated to drug trafficking, arms trafficking, human trafficking, etc., whose fundamental objective of these organized power groups is illicit profit. (Alvarez, Llorente, Cajiao, & Garzón, 2017, pág. 14)

Another of the basic points of this structure is the cohesion among the members of the organization, due to a culture of power and respect for codes of conduct, which implies the fact of staying united in all criminal activities, by virtue of the fact that when performing each of these acts, everyone is responsible in the various degrees of participation, reason why, they have the obligation to remain



silent when being questioned by the corresponding Police Agency, by virtue of the fact that in these criminal networks, there are groups of lawyers dedicated to criminal technical defense.

Unconditional obedience to superior orders is of paramount importance for the criminal structure to remain properly organized and hierarchical for the fulfillment of its purposes. The use of violence and intimidation for the execution of their objectives is vital, because instilling fear in the population or in their victims implies the fact of unconditional obedience to their orders and the fulfillment of their objectives.

The activities of these transnational criminal organizations that are directed from a specific center of operations, and are executed in other territorial districts, in which they have in one way or another the management of the structures of administration of justice, such as judges, prosecutors or public defenders, as well as politicians that allow them to operate without any kind of impediment, It is another of the important points within the basic elements of organized crime, since by virtue of the high profits, it would imply distributing them among people who are part of the criminal group, or those who are on the payroll for monthly payments and that allow them to give both legal and political protection to those who execute this kind of activity, Known today as "narco-states".

#### **Aims of organized crime**

For the fulfillment of the purposes, organized crime establishes commercial and economic structures that allow it to manage money from an effective point of view when investing the profits obtained from illicit activities, which is why these criminal networks work horizontally in favor of organized crime structures, For example, when dealing with the trafficking of controlled substances in which we have the production, transfer, marketing, and delivery of the drug, but which definitely needs other criminal groups for the execution of their purposes, such as criminal enterprises dedicated to hired assassins that give protection to the collection and transfer of the alkaloid, or, failing that, those companies that are dedicated to money laundering, that is, to reinsert into the financial torrent all the profits obtained illicitly, and that by investing them in lawful businesses, their profits would be legal.

In this sense, we can explain that most criminal organizations, whether small or large, are generally linked to the exercise of violence as well as intimidation or extortion in a certain territory, with the purpose of obtaining economic or legal benefits through the threat to officials.

#### **Cybercrime**

Computer criminals carry out their acts in cyberspace, which is a totally different area from the place where other illegal acts consummated by conventional crime are carried out. Cybercrime uses information and communication technologies and virtual space as a place for criminal injustice.

Therefore, the denomination of cybercrime "perfectly expresses the concern for a new type of crime that emerged with the appearance of the first computer systems, in which these were the means or the objective of crime". (Miró Llinares, 2011, pág. 3)

At present, cybernetics "has become a new form of operation within the structures of organized crime, to facilitate their traditional activities" such as: trafficking in narcotic substances, which from the administrative point of view allows the organized management of said criminal enterprise, thus establishing logistics, organization and direction through information and communication technologies, and when it comes to the execution of conduct linked to cybercrime, such as hacking, sabotage or computer espionage, it can be established that it serves as a means to a specific end, such as the attack on the official database of the State with the aim of preventing its structure from being identified, or steal sensitive information for other purposes, such as extortion, blackmail, industrial espionage. (Flores, 2022, pág. 10)

Therefore, in this technological era of the fourth industrial revolution, attacks are no longer aimed at computers or equipment that store relevant information for the owner, but those integrated information systems which travel through cyberspace, the same "that is capable of communicating and allowing communication as well as generating vital information both personal and economic", financial or any other nature that makes information one of the main assets at this time. (Perez, 2021, pág. 176)



## DISCUSSION

In this research it was possible to find several issues that contribute to the construction of this paper and that explain the reason for the vertiginous development of each of the criminal organizations in their field, thus enunciating the concept of gray zone of a State which is used to designate "those geographical spaces where there is no law of any State, with diffuse and lasting crisis scenarios, which aims to establish in certain regions or urban or rural areas the control of certain criminal groups" through acts of violence and threats, because they have come to be controlled by a criminal organization of that territorial circumscription or another with transnational command networks. (Torres Vuelvas, 2019, pág. 330)

So we can also observe how organized crime is embedded and infiltrated in the powers of a State, whose purpose is the management with public policies that benefit these organized groups and in this way "capture the State by organized crime through acts of corruption, which outline the success of criminal organizations, for the ease in the execution of its purposes and the help of the public servant". (Rincón, 2018, pág. 68)

Organized crime at this point benefits from that underground economy and legal loopholes that allow public policies managed by the government, as well as corruption and violence that is embedded in the different powers of a State and its agencies and institutions of public power, in order to benefit economically from "the income of the illicit business, the surreptitious use of political power, the consolidation of transnational illicit networks, as well as the expansion of violence in areas where illicit trafficking is produced." (Umbría, 2018, pág. 248)

Organized crime is attributed to the production of conditions of citizen insecurity, since its members do not offer a minimum guarantee of cognitive security that is necessary for people who act in law to develop in society, so they are not treated as people but urgently as enemies. (Gutierrez, 2019, pág. 370)

Cybercrime has evolved adapting to the digital age today, so for example we have the "pickpockets or punguistas", a method that was evolved into the form of online robberies and the activity of the so-called Calders, who use the network to commit identity theft and fraud through credit cards (Cata del Palacio, 2014, pág. 41).

Technological advances in this digital age have allowed agents to use this class of cyber attacks such as the use of the Botnet virus, which constitutes "a network of computers connected and infected by malware programs that are often used by attackers to launch distributed denial of service attacks", to explore new techniques that improve their tools and attack methods. thus providing a different vector for the cybercriminal to carry out various criminal operations in which it would be almost impossible to discover him, such as: the misappropriation of money through virtual or electronic banks that the institutions of the financial system have for this purpose; the application of ransomware malware that is nothing more than the hijacking of information; Cryptocurrency mining and denial of service attacks that saturate the system in order to disable all security measures for a smooth entry into the system. (European Union Agency for Cybersecurity, 2019, pág. 1)

Cybercrime has become immensely attractive to the transnational organized crime that lives in it, a perfect instrument for expanding its enrichment and influence worldwide complementing its well-known traditional activities. (González, 2017, pág. 2)

## CONCLUSIONS

In view of the present investigation, the following conclusions have been reached:

Organized crime is structured with the purpose of a large-scale criminal concertation, with different criminal networks at its service and that depend directly on this organization.

The execution of acts in organized crime is much more visible, since they are executed in a material way through the use of violence and threat to the fulfillment of the ends, being more perceptible to the senses.

The hierarchy of a criminal structure is of capital importance in organized crime, in order to maintain control over the criminal enterprise.





Cybercrime is part of a new criminal paradigm, since its consummation is executed in cyberspace, and that this virtual territory, although it is true that we can all access, its form of alteration, manipulation or modification of computer data as such for the execution of attacks, requires technical knowledge of the agent.

In this kind of virtual crime there is no need for an organized power structure that manages the cybercriminal, rather it has been observed that they are independent people in the execution of the unjust computer criminal.

It has been established that cybercrime is not a criminal network of organized crime, dependent on it, but rather a group of independent technological criminals who venture into another kind of platform, such as cyberspace, and who would provide their illicit service in response to supply and demand.

## REFERENCES

- [1] Alvarez, E., Llorente, M. V., Cajiao, A., & Garzón, J. C. (2017). Organized crime and armed saboteurs in peacetime: X-ray necessary. Bogota: Ladoamable Ltda.
- [2] BOE. (2019). National Cybersecurity Strategy 2019. Madrid: Boletín Oficial del Estado.
- [3] Cata del Palacio, A. (2014). Cybercrime: Development and technological persecution. Polytechnic University of Madrid. UPM Digital Archive , 1-182.
- [4] European Union Agency for Cybersecurity, (. (January 20, 2019). European Agency for Cyber Security. Obtained from ENISA: <https://www.enisa.europa.eu/events/botnets>
- [5] Flores, J. (2022). Cybercrime as a commission modality of the crime of trafficking in persons and its criminal legal treatment in Nicaragua. . Criminological constructs, 9-30.
- [6] Gimenez-Salinas Framis, A. R. (2011). Is there an organized criminal profile? Exploration from a Spanish sample. Electronic Journal of Criminal Science and Criminology., 3-32.
- [7] Gonzalez, M. (2017). Cybercrime as an instrument for the expansion and empowerment of organized crime. GESI International Security Study Group, 1-24.
- [8] Gutierrez, O. (2019). Organized crime in the light of the enemy's criminal law. Journal of Research in Law, Criminology and Legal Consulting, 367-393.
- [9] Lusthaus, J. (2018). Is te mafia taking over cybercrime? En U. 2. Black hat (Ed.), Ciclo de conferencias Black hat, USA 2018; August 4-9 (págs. 1-11). Mandalay Bay-Las Vegas: Black hat, USA 2018. Obtenido de <https://www.blackhat.com/us-18/briefings/schedule/#is-the-mafia-taking-over-cybercrime-11177> ,
- [10] Miró Llinares, F. (2011). The criminal opportunity in cyberspace. Application application and development of the theory of everyday activities for the prevention of cybercrime. Electronic Journal of Criminal Science and Criminology RECPC, 1-55.
- [11] United Nations Organization. (2004). United Nations Convention against Transnational Organized Crime. New York: UN.
- [12] Perez, J. (2021). Cybercrime: Towards a new virtual-reality of Criminal Law. International Journal of Doctrine and Jurisprudence, 175-193.
- [13] Rincón, D. (2018). Corruption and State Capture: The criminal responsibility of public servants who take part in organized crime. Revista Prolegómena - Derechos y Valores, 55-71.
- [14] Rodríguez-Barrigón, J. M. (2011). Euro-Latin American strategic relations and organized crime. Yearbook of the Faculty of Law University of Extremadura, 151-173.
- [15] Sanchez, C. (2012). On the concept of organized crime. Significance of its content in Salvadoran criminal legislation. . Journal of Politics and Public Security, 29-62.
- [16] Torres Vuelvas, J. (2019). Gray areas and transnational organized crime: challenges to state sovereignty in Latin America. Revisra VIA IURIS, 318-349.
- [17] Umbria, L. (2018). A preamble to criminal policy against organized crime. Criminal Review, 235-249.