Revista Iberoamericana
de las Ciencias Sociales y
Humanísticas

RICSH

ISSN: 2395 - 7972

https://doi.org/10.23913/ricsh.v8i16.179

Artículos Científicos

Perfil psicosociológico en el ciberdelincuente

Psychosociological profile in the cybercriminal

Perfil psicossociológico no cibercriminoso

Juan Carlos Fernández-Rodríguez
Universidad Antonio de Nebrija. Madrid, España
jfernanr@nebrija.es
https://orcid.org/0000-0003-3312-861X

Fernando Miralles Muñoz
Universidad San Pablo CEU, España
f.miralles@ceu.es
https://orcid.org/0000-0003-3382-5343

Luis Millana Cuevas
Universidad Antonio de Nebrija. Madrid, España
lmillana@nebrija.es
https://orcid.org/0000-0002-7824-6313

Resumen

En el presente artículo se estudian las características más importantes de los conceptos que hoy conocemos como *ciberdelincuencia*, *ciberterrorismo* y *ciberguerra*. En relación con la ciberdelincuencia y el ciberterrorismo, se proporcionan datos sobre los posibles perfiles existentes y sobre distintos arquetipos de personas que tienen estas conductas delictivas. En lo concerniente a la ciberguerra, y debido al reducido número de estudios planteados sobre este fenómeno, se exponen los datos más relevantes sobre este hecho y se resalta la falta de estudios para describir a sus actores desde un prisma de carácter psicosociológico.

Palabras clave: cibercrimen, ciberdelincuencia, ciberguerra, ciberterrorismo.

Abstract

In the present paper we study the most important characteristics of the concepts that we know today as cybercrime, cyberterrorism and cyberwar. Regarding cybercrime and cyberterrorism, data are provided regarding possible profiles and also about the different archetypes of people who perform these forms of criminal behavior. Regarding the cyberwar, and because of the small number of studies on this phenomenon presented the most relevant data on this fact and highlights the lack of studies that describe their actors from a prism of psychosociological character.

Keywords: cybercrime, cybercrime, cyberwar, cyberterrorism.

Resumo

Neste artigo, estudamos as características mais importantes dos conceitos que conhecemos hoje como cibercrime, ciberterrorismo e guerra cibernética. Em relação ao crime cibernético e ao ciberterrorismo, são fornecidos dados sobre possíveis perfis existentes e sobre diferentes arquétipos de pessoas que têm esses comportamentos criminosos. No que diz respeito à guerra cibernética, e devido ao pequeno número de estudos levantados sobre esse fenômeno, são apresentados os dados mais relevantes sobre esse fato e destacam-se a falta de estudos para descrever seus atores a partir de um prisma de natureza psicossociológica.

Palavras-chave: crime cibernético, crime cibernético, guerra cibernética, ciberterrorismo.

Fecha Recepción: Marzo 2019 **Fecha Aceptación:** Julio 2019

Introduction

In the global technological society, cybercrime is a phenomenon that has increased considerably in recent times. This happens in the middle of a context where people are increasingly dependent on information and communication technologies (ICT), hence it is necessary to increase the standards in digital security to prevent potential cybercrimes that can not only affect individuals, but also companies, organizations and governments.

In 2015, for example, 81,307 crimes were registered, of which 74.4% were related to computer fraud (scams), while 13.9% were linked to threats and coercion (Ministry of Interior, 2017). Also, in 2014, more than 317 million new malicious codes (Trojans, worms, viruses, etc.) were registered, that is, almost one million threats issued per day in cyberspace (Symantec Corporation, 2015, cited by Guilabert, 2016).

An emblematic case of cybercrime was that carried out by engineer John Draper, who was arrested in 1972 for fraud against telephone companies. As it is known, it all started when a blind friend of Draper (Joe Engressia) told him that obstructing the air outlet of one of the whistle trades that a famous company (Quaker Oaks) added in its cereal boxes could generate a tone 2600 Hz pure, frequency that was equal to the tone made by the telephone system to warn the conclusion of a call.

Once the 2600 Hz tone was emitted, one of the ends of the line was disconnected and the connected side entered into operator mode, whereby the special tones that defined the call could be “heard”. This helped Draper to devise an apparatus that imitated different tones registered by the switchboard, so that he could control and modify his behavior for his own benefit. The production of this device, known as blue box 35 or blue box, became the first major case of the so-called phreaking or telephone hacking. This strategy of Draper was used by a large number of users, who were able to make free long-distance telephone calls, which not only caused great losses to the telephone companies, but also collaborated with the rise of the hacker movement.

This event caused great enthusiasm in electronic engineering universities; in this way he came to be known by Steve Woznkiak, a talent of that discipline, who began to reproduce those boxes to sell them and get capital with his partner Steve Jobs.

Another example of these electronic crimes was the great cyber bank robbery carried out in February 2016; This consisted of the extraction of 81 million dollars from the central bank of Bangladesh, which were deposited in the Federal Reserve Bank of New York City. This crime was materialized thanks to malware that reproduced legal transfers of funds through an application called SWIFT, which is used by all banks to carry out operations between them (Leetaru, 2016).

Objective

It is common that in different media - whether specialized or not - different expressions or words are used, but with different meanings, which can alter not only the meaning of the information to be transmitted, but also the way in which it is interpreted by the receiver, hence it is necessary to explain them in greater detail. Due to this, the objective of the present work is to seek a clarification of terms such as cybercrime, cybercrime, cybercrime and cyber terrorism, as well as expose the most outstanding psychosociological qualities of these phenomena and the possible classes of criminals according to the mentioned categories.

Methodology

To meet the above objectives, a bibliographic search has been carried out, which was completed in February 2019. The terms used as keywords were included in that process. The results have been restricted to the information collected in the Spanish language.

Results

The terms cybercrime and cybercrime are used quite regularly to refer to similar situations. In fact, and following Roca (2014), cybercrime is associated with those illegal activities that are executed through the use of current communication and information systems. According to the Dictionary of the Royal Spanish Academy (RAE), the word crime has three meanings: 1) guilt, breaking the law; 2) action or reprehensible thing, and 3) voluntary or reckless action or omission punishable by law. These three meanings can be transferred to crimes committed through ICT. Likewise, the word crime is linked to a "set of crimes", hence it is possible to associate it in the appropriate fields with the term cybercrime. The same usually happens with the word cybercrime.

According to the RAE, crime is the "voluntary act of killing or seriously injuring someone." Therefore, it does not seem a concept that can be applied to the world of communications, although it is correct to use the first meaning referred to because a crime is not only a “serious crime”, but also an “improper or reprehensible action”, which is It can move to the virtual environment of computer science and communications.

For Miró (2012,), cybercrime or cybercrime is any crime in which ICT “plays a decisive role in its specific commission, which is the same as affirming that it will be any crime carried out in cyberspace, with the criminological particularities , victimological and criminal risk arising from it ”(p. 44). According to this position, the terms cybercrime and cybercrime seem to be used interchangeably (in the case of cybercrime, it refers to all criminal actions carried out in cyberspace). In this sense, the words cybercrime and cybercrime can be considered synonymous (as a concrete action: "Cybercrime has been committed").

Now, from a psychosocial perspective, terrorism is linked to a way of creating chaos and anxiety in the civilian population (Fernández-Rodríguez and Miralles, 2016). This form of violence, transferred to the world of cyberspace, gives rise to the so-called cyberterrorism, a form of crime that materializes on the Web not only by traditional terrorist organizations that rely on their religious beliefs to comment on different punishable acts, but also by new groups or organized gangs of cybercriminals that promote political or ideological protests and whose members are known as hacktivists (Mateos, 2013).

Cybercrime and cybercriminals

The so-called cybercrime has expanded based on the development of new technologies, a well-established space without borders in which a series of vandalism acts can be committed without the restrictions imposed in the traditional environment. This has required the emergence of an information society that focuses on prevention, investigation, evidence and repression of the criminal act, overcoming the obstacles presented by the jurisdictions of the different countries.

In this regard, however, it is worth mentioning that the great challenge of criminal justice in the democracies of today is to reach a balance between security and individual freedoms so that the guarantees of citizens are not sacrificed (French, 2005).

To have a broader view of cybercrime in Spain, it is necessary to refer to the report on that phenomenon in that country corresponding to 2017 and published by the Ministry of Interior (Ministry of Interior, 2017). For the drafting of this report, the statistical information collected on known crime was taken as a source, which is recorded by the different security forces and bodies (National Police, Civil Guard, Foral Police of Navarra and multiple local police bodies). This information can be found in the Statistical System of Crime (SEC) and in the National Center for Critical Infrastructure Protection (CNPIC). This report incorporates an x-ray of the information society, as well as other types of statistical data, such as the number of detentions / accusations, the facts known by criminal categories, the territorial distribution of cybercriminality, the profile of the victim and of the person in charge, the incidents registered by CERTSI, etc.

In addition to this, figures are added around the way in which Spanish society in general uses technologies, as well as comparisons between those uses and those made by other states in our environment. This type of results is obtained thanks to surveys and opinion studies carried out by different organizations both at national level (National Institute of Statistics of Spain [INE]) and European (Eurostat). Some of the most outstanding data are the following (Ministerio del Interior, 2017):

a. The total number of arrests or persons investigated by the State's security forces and forces was 4912, of which 77.04% were men.
b. From the analysis of the different criminal typologies included in this report, among the detained / accused men, threats, scams, child pornography stand out, as well as the discovery and disclosure of secrets; while threats, scams, insults and the usurpation of marital status are predominant in women detained / charged.
c. Most of those arrested / charged with cybercrime are Spanish (84.6%), while those arrested / charged in other countries are predominantly Romanian, Moroccan (also occurs with victims), Nigerian, Colombian and Ecuadorian. The group of detainees / defendants between 26 and 40 years of age frequently executes the crimes of threats, computer fraud and coercion. As for minors, there is a preponderance in crimes of threats, coercion, access and illegal interception and sexual crimes.

According to Mateos (2013), there are a large number of studies that suggest that the typical profile of the cybercriminal corresponds to a male person, between 25 and 35 years of age and with certain technological and computer skills that empower him to use the Internet as a perfect formula to execute its activities, although it is worth mentioning that the age of onset in cybercrime is decreasing, so you must study what are the precipitants of this fact (González and Campoy, 2018).

A cyber criminal or hacker, in general, distrusts the authority (which he usually considers oppressive) and believes that access to all types of information should be free and unlimited; However, it is necessary to know that these types of criminals have characteristics and behaviors that serve to offer different categorizations, as explained below. (Mateos, 2013):

a. *White hat hacker:* Usually known as traditional hackers or ethical hackers. Its greatest evil is to leave a business card to inform the system administrator of the failures and vulnerabilities found after an attack or entry into your system, or making - in the worst case - only some modifications to achieve anonymity. In some circumstances, the white hat hacker are people who have belonged to the black hat hacker, but who decided to modify their malicious determinations to fight cybercrime and support the administrators of security systems. The terms black hat and white hat come from the old western movies where the good ones wore white hats and the bad guys always wore a black hat (Meseguer, 2013).

b. *Black hat hacker*: Those who are commonly referred to as regular hackers. They are identified because they do not follow any ethics and because they seek economic and personal benefit. The black hacker tries to collapse servers, penetrate prohibited areas or take control of systems and networks. In this case, however, some exceptions can also be referred, as happened with a Russian hacker who in an important forum expressed his discomfort and dislike for those who attacked public health systems. Indeed, in the Russian clandestine circles there is a certain "ethical code" that leaves these assistance centers out of such attacks, regardless of whether they are in countries that are usually targeted by their campaigns and cyber attacks (McAfee, 2016). These people feel proud when they demonstrate their abilities, so that their degree of self-realization is higher when the impact of the damage caused is greater.

c. *Gray hat hacker:* They are subjects with an ambiguous ethic. These people have knowledge comparable to those of a black hat hacker, although they also use them to locate vulnerabilities or security flaws, which are used to later offer a solution in exchange for financial compensation.

d. *Cracker*: They could be included in the group of black hat hacker. They are taken as the most aggressive and perhaps most dangerous group. Its sole objective is to "burst computer" or electronic systems. The cracker have great programming experience and use their knowledge to modify the behavior of networks and systems, taking advantage of any vulnerability found. They act in an almost insatiable and obsessive way, directed by their destructive and egotistical eagerness.

e. *Lammer*: Rejected within the hacker collective, they are subjects that are dedicated to collecting information and executing malicious codes seeking social recognition as a hacker without having a real knowledge of the impact of their actions or the functioning of the code executed. They can be a nuisance, although their actions do not usually cause serious damage.

f. *Phreaker*: Collective dedicated almost entirely to the world of telephone systems, including mobile telephony and voice over IP (VoIP). They have a great knowledge of the operation of these technologies and their communication protocols, so they are dedicated to altering the behavior of the systems, sometimes for pleasure and sometimes for economic purposes.

g. *Scriptkiddie***:** They are simple Internet users who are interested in hacking issues, although with a shallow knowledge. They can use programs or malware that they download from the Internet and run without further knowledge or study, so in some cases they can infect their own systems.

h. Wannaber: They are aspiring hackers with low technical capacity and little perseverance, which in most cases make them harmless. They usually use their low computer skills to obtain social prestige outside the Network.

i. *Newbie*: They are known as hacker learners. They are novice users who start reading and experimenting with the information found. Sometimes they make incursions into weak systems but without major importance due to their limited knowledge in the area. Normally your only goal is to learn.

j. *Hackers*: This denomination is usually confused with that of the term hacker. However, hackers only engage in the illegal copying and distribution of software, music, games and other content, thereby infringing intellectual property and the rights of their owners.

k. *Buccaneers*: They play the role of merchants in the Network. They are dedicated to buying and selling illegal material obtained through others, such as identities, access control cards, cracked software, etc.

From the above, it can be indicated that a cyber criminal is anyone who can be accused of exercising cybercrime or cybercrime. Similarly, those subjects whose illegal activity has evolved with technology, such as pedophiles, pimps, etc., are considered cyber criminals.

In addition to this - and although the characteristics of the different types of hacker or cybercrime subjects have been named - it may be considered relevant to add some additional profiles that have emerged today, which can be found in different technological articles , among which are the Report on Virtual Criminology of the McAfee computer security company, which are explained below. (McAfee, 2009, citado por Mateos, 2013):

a. *Bot installers:* Those users who seek to gain control of a remote computer thanks to the installation of malicious software. To achieve these purposes, they use a preprogrammed malware, which is embedded in a hidden way in all kinds of interactions that the user makes while browsing the Web.

b. *Carders:* This class of cybercriminals focus exclusively on identity theft and the achievement of fraud through credit cards on the Web. Carders, therefore, can be considered as a virtual evolution of traditional street pickpockets. Once the necessary information has been achieved, they can make transactions and purchases online covering up their identity and charging the cost to their victim.

c. *Cyberpunks:* Without having a lucrative objective in their actions, cyberpunks - denomination arising from the literary movement with the same name - can generate great losses to their victims both economic and image. Considered as the naughty cyber criminal, cyber punk is dedicated to altering public systems - like a web page - to mock and ridicule different users.

d. *Insiders:* They are employees or former employees who act from within the companies in which they work or have worked to access, distribute confidential information or otherwise harm their companies. Their motivations are usually both economic and personal, even for revenge.

e. *Phisher, spammer:* Users specialized in using email as a way or means of communication with their victims. They try to achieve an economic benefit through deception and decoys that confuse clueless cybernetters, who are shown to be apparently reliable sources.

The individual who commits this type of punishable acts is not considered a common criminal, since it differs from the latter in the mechanism and in the means used to produce the result. In this sense, it is important to mention that there is no individual profile to describe these cybercriminals, although attempts have been made to extract a series of common characteristics (Garrido, Stangeland and Redondo, 2006). In other words, it can be affirmed that people who commit these criminal behaviors have certain traits that traditional criminals do not have, that is, they have high skills in the management of computer systems and usually in their workplace enjoy information of a character sensitive (Gallego, 2012).

In accordance with this idea, and according to research carried out at Yale University to study the characteristics of cybercriminals, it has been shown that people who commit computer frauds meet the following characteristics: the majority are older, married and older men. economically stable because they have a fixed job. In addition, they have a high level of education, good self-esteem and are not considered criminals (Garrido, Stangeland and Redondo, 2006, cited by Dinca, 2016). Likewise, and taking into account the criminological studies that have taken care of studying the profiles of these criminals, it can be said that they have minimal knowledge of the computer environment, without which they could not access the different systems (De La Cuesta y Pérez Machío, 2010).

Another characteristic that makes new technologies attractive to cybercriminals, especially to commit cyber attacks of different types, is the massive effect they could achieve with their actions. For example, with the use of Trojans on thousands of computers, attacks can be carried out simultaneously with really serious consequences. The unfortunate and paradoxical of this action, however, is that in many cases it is very difficult to point to the author of the attacks, since there are techniques that allow camouflaging and hiding to some extent the direction of some teams (Roca, 2014).

A particular type of cyber criminal is one that operates from within companies. These may not be experts in technology, but they know the vulnerabilities in the technological security of an organization, which is used to get the data they are looking for. Among these criminals are the insiders, who can be executives who change jobs and take with them in any storage device the database of the clients with whom they have worked (Portafolio, 2013). Here are some of these cases:

a. People with user and network knowledge that constantly use computers without explaining what they do and without sharing that knowledge. These may even disparage others for their computing competence.
b. Employees who work overtime for no apparent reason, who do not enjoy vacations or who do not make frequent use of computers, but who suddenly start using them for no reason.
c. An alert situation occurs when people whose work duties are not related to computers (eg, cleaning managers) are in the offices using them.
d. Subjects that take advantage of social spaces to be interested in customer data and other information of restricted or particular use.
e. Personnel who install spyware without authorization from the organization.
f. Subjects that disable antivirus software on work teams.
g. Persons who, without authorization, use computers or devices of the other members of the organization.

h. People without experience, but who have the knowledge about the vulnerability of certain points in the technological security of the company, which take advantage to get the data they need.

Following the study of Digiware (Gallo, May 3, 2016), cybercriminals no longer act in isolation, because in many cases they operate for large criminal organizations around the world, which attack about 600,000 times day, especially to the financial sector and governments. According to Digiware, half of the cybercrime gangs are usually made up of six or more people, of which 76% are men whose ages range between 14 (8%) and 50 years (11%), with an average of 35 years (43%). On this aspect, it should be noted that about half of the cybercriminals have carried out these operations for more than six months, while 25% have done so for half a year or less. These activities are mainly carried out in North and South America, with 19% of total attacks worldwide.

Digiware also asserts that the majority of attacks carried out within companies are committed by a hacker in a premeditated manner and with direct intervention in the internal systems of organizations. These accesses in 9.3% occur due to the negligence of the employees and in 7.3% due to accidents of the members of the company. Digiware emphasizes that attacks on brands are the most used by criminals to reduce the value of the shares or to seriously affect the image of companies through fraud towards their customers. Also, we try to interrupt digital services, such as blocking access to emails or hacking websites. About these actions it is worth commenting that they have different rates; for example, $ 25 for the theft of a Skype account or $ 200 for accessing data on social networks or extracting professional information.

In short, anyone with sufficient computer skills and driven by economic anxiety can lend their work to security companies or use it for their own benefit. Likewise, it is also worrying that the profile of these black hats is associated more frequently with young people and, mainly, minors, which limits the fact that they assume the consequences for their acts, since the criminal responsibility of minors (in the case of Spain) people over fourteen years of age and under eighteen are required for the commission of acts classified as crimes or offenses in the Criminal Code or in special criminal laws.

In this context, it should be added that it is still difficult to draw a unique profile of the cyber-offender, which can be explained by the intimate relationship that the cyber-aggressor shares with the cybercrime, an issue to which the difficulty of judicial prosecution of This type of criminals. In addition, it should be noted that the lack of criminological, quantitative and qualitative studies on specific profiles does not contribute to offering a single general conclusion (Miró, 2012).

For example, and following Di Piero (2012) in the case of the economic cybercriminal, this profile does not correspond with that of an individual and concrete person, but with that of a criminal organization, the hacker being the paradigm of this cybercrime. who explains the transformation he has suffered.

In the case of political cybercriminality, the different organization that it presents in relation to the criminal agents of the physical world stands out, with an emphasis on its horizontal, not vertical organization, with a central objective to which different subjects who participate in ideologies without that there is a high technical knowledge of necessary and, therefore, expendable. Likewise, the possible individual action outside of any organizational relationship is not ruled out. Finally, social cybercriminality may be the most complex due to the existence of multiple motivations in the active subject, although always with the uniqueness that cyberspace gives it.

Cyberterrorism and cyberterrorists

Although several scholars consider that both terms are comparable, cyberterrorism transcends cybercrime. In fact, although it is true that in several aspects these words have a certain semantic link, because on many occasions cyberterrorists carry out criminal activities on the Web, the causes that motivate their actions and the benefits they expect to receive from each other are different.

Cyberterrorism is the confluence of terrorism and cyberspace, that is, the way in which terrorism uses information technology to coerce, intimidate or harm social groups for political-religious purposes. In other words, it is the evolution that results from exchanging weapons, bombs and missiles with a computer to plan and execute attacks that produce the most serious damage possible to the civilian population. Cyberterrorism, therefore, seeks to cause as much damage as possible for normally political-religious reasons, while cybercrime actions are aimed at obtaining a benefit mainly of an economic nature (Sánchez Medero, 2012).

How can the cyberterrorist be known? Due to his knowledge of the technique, in principle he could be considered as a person with a high IQ, but this observation could be wrong, because the cyberterrorist can act even without having an excellent profile in the management of information technology. Therefore, the ideas of Patron (2013) are illustrative, who explains some qualities of the computer terrorist:

a. He is a person who through his actions causes panic and terror in order to weaken and discredit governments, society, a belief, etc.
b. He is a subject with a strategic character, since he is able to capture both the attention and support of the community (colleges, universities, churches, etc.). In this case, it uses computer media and social networks.
c. It is a subject that has clearly marked its objectives of both attack and target population (target audience).
d. His criminal profile is far from the "white collar criminal" parameter, as noted by American sociologist Edwin Sutherland (1943) to refer to a computer criminal. With the advance of the times, to think that only people with high purchasing power can be cybercriminals is to make a clear mistake before the world perspective and its progressive advance. Anyone can be trained to be a computer terrorist or to design web pages, because you only need a computer and the intention to learn.
e. He is a person with a strong resentment towards society or a group within it, a key element for terrorism in many cases.
f. Finally, know the ways to attack using different computer means. This point is understood as knowing what programs to manage, how to capture people through computer means and how to reach their various purposes with the use of the Network.

Cyber war

Before specifying what cyber war is, you must establish your differences with cybercrime. The latter focuses on attacking to achieve economic retribution or causing damage to victims without taking into account any activist ideology (Pantano, 2014). Cyberwarfare, on the other hand, can be defined as a type of aggression promoted by a State and aimed at seriously damaging the capacities of another State to impose the acceptance of its own objective, to appropriate certain information or to alter or destroy its communication systems and modify their databases. In short, cyberwar is linked to what is traditionally known as war, but with the fundamental difference that the means used would not be physical violence, but a digital attack that goes from “infiltration into enemy computer systems to obtain information to projectile control through computers, through operations planning, supply management, etc. ”(Colle, 2000, Computer war, para. 4). Cyberwar, then, involves the use of all electronic and computer tools to tear down the enemy's electronic and communication systems and keep their own means operational (Sánchez, 2008).

Undoubtedly, the battlefield of cyber war is cyberspace, where the elements of power are established. It is an area in which the beneficiary is the one who takes the initiative. The opportunity for action, response and counter-response are variables of imbalance in deterrence, where inaction facilitates the escalation of aggression by those who seek the asymmetric effect as an action strategy (Arteaga, Ballesteros, Cerpa, Cervantes and Díaz, 2019). For this phenomenon, due to its special characteristics, no data have been found on the profiles of its different actors.

Conclusions

The Internet has become a perfect space for the implementation of cybercrime and cyberterrorism, as it is not usually regulated by any well-defined laws. In addition, these criminal practices can be developed anonymously and with a very high impact that can be achieved with little investment and risk for those who commit the crime. In this sense, it is worth emphasizing that despite the work done by the agencies or security secretaries of the States, it is very difficult to guarantee the integrity of the computer systems.

Obviously, regulatory actions such as those imposed in some countries such as China, North Korea or Saudi Arabia, which, paradoxically, have been frequently accused of carrying out cyber attacks can be implemented. Also, you could choose not to connect to the Internet, although this would be almost unthinkable today because many of the daily activities are carried out thanks to that digital medium. Therefore, it seems that the most viable option would be to identify vulnerabilities and potential hazards to strengthen computer systems. However, the increase in communications control or the creation of specific agencies (cybervigilants) do not seem to have positive results so far.

In addition to this, and according to the revised documentation, so far it is complex to describe the specific profile of cybercriminals and cyberterrorists, since the information available only serves to offer a simple description of general and inaccurate characteristics, which is insufficient to control or prevent the activity of these people in the Network.

In any case, as described throughout this work, cybercrime, cyberterrorism and the States are turning to the Web to exercise, extend and develop their activities although, of course, with different objectives and purposes.

Cybercriminals use the Network to damage and block in order to achieve economic profitability or achieve their interests outside the law. In this sense, terrorist groups are moving their diffuse organizations to cyberspace because that way they can be diluted in a place where the authorities find it more complex to act. In this way, they use the Network to finance themselves, recruit other people, train, communicate, coordinate, indoctrinate, get notoriety, etc.

In this context, cyberspace has become a battlefield with new possibilities for criminals, since this type of aggression is usually characterized, unlike traditional warfare, for its great asymmetry, short duration, rapid reaction, low economic costs and lower physical damage for soldiers. Cyberwarfare, therefore, is a way to fight intensely not to physically bend the adversary, but to dominate rival systems from almost anywhere and almost undetectable. This means that for cyberwarfare it is not necessary to have a sophisticated weaponry, a large army and be located near the enemy, because it is enough to possess a computer and certain computer skills to achieve effects as devastating as those achieved with traditional warfare. However, despite these possibilities to generate damage in the rival, it should be noted that at the moment both countries and terrorist groups appear to be making passive use of the Network, except for the propaganda resources used by the Islamic State, others related groups or cybercriminals.

In the midst of these circumstances, the annual report of the McAfee security company is alarming, in which the possibility of having to face a “cyber cold war” has been envisioned. This means that cyberwar, cybercrime and cyberterrorism are real threats to which attention should be paid throughout this 21st century.

For this, it is essential that each user of the Network tries to ensure that the information they want to transmit reaches the chosen destination and is used correctly or for the desired purpose. This implies adopting best practices in cyberspace, as well as using more powerful antivirus and keeping the software used on the Internet updated. Therefore, it should be aware that cyber criminals can be found on the lookout for any victim, be it a person, an organization or a State.

References

Arteaga, M., Ballesteros, M., Cerpa, O., Cervantes, D. y Díaz, H. (2019). *El pensamiento estratégico: una habilidad para anticiparse al futuro.* Chile: Centro de Estudios Estratégicos CEEAG. Recuperado de http://www.ceeag.cl/wp-content/uploads/2019/03/40603-TICA-3-EL-PENS-EST.pdf#page=88.

Colle, R. (2000). Internet: un cuerpo enfermo y un campo de batalla. *Revista Latina de Comunicación Social, 30.* Recuperado de http://www.revistalatinacs.org/aa2000qjn/91colle.htm.

De La Cuesta, J. L. y Pérez Machío, A. I. (2010). Ciberdelincuentes y cibervíctimas. En De La Cuesta, J. L. y De la Mata, N. J. (eds.), *Derecho penal informático* (pp.99-120). Navarra: Civitas Ediciones-Thomson Reuters.

Di Piero, C. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Recuperado de http://www.indret.com/pdf/984.pdf.

Dinca, C. F. (2016). *Fraudes en internet* (trabajo final de grado). Universidad Jaime I de Castellón (España). Recuperado de http://repositori.uji.es/xmlui/bitstream/handle/10234/161252/TFG_2016_DincaClaudia.pdf?sequence=1.

Fernández-Rodríguez, J. C. and Miralles, F. (2016). The terrorist suicide woman in Jihadism. In Martín Ramírez, J. and Fernández-Rodríguez, J. C. (eds.), *Security in Infraestructures* (pp. 186-202). Newcastle: Cambridge Scholars Publishing.

Gallego, A. (2012). *Delitos informáticos: malware, fraudes y estafas a través de la Red y cómo prevenirlos* (proyecto fin de carrera). Universidad Carlos III de Madrid. Recuperado de http://e-archivo.uc3m.es/bitstream/handle/10016/16868/pfc_alberto_gallego_yuste.pdf?sequence=1.

Gallo, T. (3 de mayo de 2016). Conozca el perfil de un ciberdelincuente, según Digiware. *El Heraldo*. Recuperado de http://www.elheraldo.co/tecnologia/conozca-el-perfil-del-ciberdelincuente-258538.

Garrido, V., Stangeland, P. y Redondo, S. (2006). *Principios de criminología*. Valencia: Tirant lo Blanch.

González, A. y Campoy, P. (2018). Ciberacoso y cyberbullying: diferenciación en función de los precipitadores situacionales. *Revista Española de Investigación Criminológica*, *16*, 1-31.

Guilabert, N. G. (2016). Actividades cotidianas de los jóvenes en Internet y victimización por malware. *Revista de Internet, Derecho y Política*, (22), 59-72.

Gutiérrez, M. L. (2005). Reflexiones sobre la ciberdelincuencia hoy (en torno a la ley penal en el espacio virtual). *Revista Electrónica del Departamento de Derecho de la Universidad de La Rioja*, *REDUR*, *3*(4). Recuperado de https://dialnet.unirioja.es/revista/2206/A/2005.

Leetaru, K. (2016). *What The Bangladesh SWIFT Hack Teaches About The Future Of Cybersecurity And Cyberwar*. Retrieved from http://www.forbes.com/sites/kalevleetaru/2016/04/30/what-the-bangladesh-swift-hack-teaches-about-the-future-of-cybersecurity-and-cyberwar/.

Mateos, I. (2013). *Ciberdelincuencia, desarrollo y persecución tecnológica* (trabajo final de grado). Universidad Politécnica de Madrid. Recuperado de http://oa.upm.es/22176/1/PFC_IVAN_MATEOS_PASCUAL.pdf.

McAfee (2016). *Informe de McAfee Labs sobre amenazas. Septiembre de 2016*. Recuperado de http://www.mcafee.com/es/resources/reports/rp-quarterly-threats-sep-2016.pdf.

Meseguer, J. (2013). Los nuevos modi operandi de los ciberdelincuentes durante la crisis económica. *Revista de Derecho UNED*, (12), 495-523. Doi: https://doi.org/10.5944/rduned.12.2013.11704

Ministerio del Interior (2017). *Estudio sobre la cibercriminalidad en España*. Recuperado de http://www.interior.gob.es/documents/10180/8859844/Informe+2017+sobre+Cibercriminalidad+en+Espa%C3%B1a.pdf/a9f61ddb-3fcf-4722-b9d8-802a424a1a70.

Miró, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.

Pantano, A. (2014). *Ciberguerra.* Recuperado de https://dspace.palermo.edu:8443/dspace/bitstream/handle/10226/1448/Ciberguerra-Pantano%2068586.pdf?sequence=1&isAllowed=y.

Patrón, P. (2013). *Drogas informáticas y terrorismo informático. ¿Nuevos métodos de delito o mitos digitales?* Recuperado de http://www.derecho.usmp.edu.pe/cedetec/articulos.html.

Portafolio (2013). *Así es el perfil del ciberdelincuente en las empresas*. Recuperado de http://www.portafolio.co/tendencias/perfil-ciberdelincuente-empresas-67906.

Roca, J. (2014). *Cibercrimen y ciberterrorismo. ¿Exageración mediática o realidad?* (trabajo final de grado). Universidad Politécnica de Madrid. Recuperado de http://www.criptored.upm.es/guiateoria/gt_m078a.htm.

Sánchez, G. (2008). Ciberterrorismo: La guerra del siglo XXI. *El Viejo Topo*, (242), 15-24

Sánchez Medero, G. (2012). Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del s. XXI. *Revista CENIPEC*, (31), 241-267. Recuperado de http://www.saber.ula.ve/handle/123456789/36770.

Sutherland, E. (1943). Juvenile Delinquency and Urban Areas: A Study of Rates of Delinquents in Relation to Differential Characteristics of Local Communities in American Cities. *American Journal of Sociology*, *49*, 100-101.

Rol de Contribución	Autor (es)
Conceptualización	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Metodología	Juan Carlos Fernández: principal, Fernando Miralles: apoya Luis Millana: apoya
Software	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Validación	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Análisis Formal	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: apoya
Investigación	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Recursos	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Curación de datos	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Escritura - Preparación del borrador original	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Escritura - Revisión y edición	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Visualización	Juan Carlos Fernández: principal, Fernando Miralles: apoya Luis Millana: apoya
Supervisión	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Administración de Proyectos	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal
Adquisición de fondos	Juan Carlos Fernández: principal, Fernando Miralles: principal Luis Millana: principal