Cybercrime: A systematic review of the literature

Yasmina Riega-Viru, Dr.[1] Mario Ninaquispe Soto, Mg.[2] Juan Luis Salas-Riega, MBA.[3]
[1]Universidad Privada del Norte, Peru, yasmina.riega@upn.edu.pe
[2]Universidad Privada del Norte, Peru, mario.ninaquispe@upn.edu.pe
[3]Pontificia Universidad Católica del Peru, juanluissr1991@gmail.com

Abstract*–. These days, technology facilitates the lives of many people. However, it has also assisted crime, which presents severe threats to the assets and tranquility of those who are victims. Therefore, it is necessary to know the types and forms of cybercrime that occur in various countries of Latin America, through a systematic analysis of the literature. Sixty-two articles obtained from the Scopus, Dialnet, and Scielo databases published between 2009 and 2021 were reviewed and analyzed following the classification proposed by Miró Linares. Among the results, it was found that the highest rate corresponds to economic cybercrimes with 43%, followed by social cybercrimes with 41%, and, finally, political cybercrimes with 16%, being the malware tool the most used. It is concluded that most studies on cybercrime come from European and American countries; and that theft, the use of malware (Booter, Spyware, Trojan, Adware, Ransomware) are the main tools for committing cybercrimes, being the most recurrent: theft, cybercrime, and fraud.

***Keywords*— cybercrime, technology, digital tools, malware, script.**

I. Introduction

With the advent of technology and the transmission of information, the world has become a digital world, which facilitates communication and economic transactions; but new forms of crime are also emerging. These are crimes such as fraud or counterfeiting, the publication of illegal content, attacks against information systems, among others, which damage innovation because they divert resources to security instead of investment and impact on society because they reduce economic development. [1]

Cybercrime has no physical or geographic barriers, which means that it can be committed with less effort and more ease and speed than ordinary crimes. [2]. Consequently, it becomes a challenge for law enforcement and other security measures on the part of the government. [3]

The problem of cybercrime is addressed from two perspectives: on the one hand, law, which has a punitive perspective; its application is post-crime because its function is the repression of crime; and, on the other hand, information security, since from a technical-preventive perspective it can protect software and hardware devices trying to mitigate threats. [4]. This study aims to contribute to both areas: the first one because it identifies the context in which cybercrime takes place, whether social, economic, or political; and the second one because it identifies how the crime is carried out.

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2022.1.1.576
ISBN: 978-628-95207-0-5 **ISSN:** 2414-6390

Among the previous studies was that of Akinbowale, Klingelhofer, and Zerihun [5]. After reviewing the literature, the authors confirm a growing wave of cybercrimes that has harmed the goodwill and economic growth of financial institutions, besides the loss of confidence in the digital infrastructure. It is worth mentioning that this review addressed only the articles in the banking sector.

A. Cybercrime

At the doctrinal level, there are various definitions of cybercrime or computer crimes [6]. Cybercrime in a general context is the unlawful conduct affecting computer systems and data, besides other legal assets of criminal relevance committed using information or communication technologies. [7]. Computer crimes are seen from two approaches: for the first one, they are just conventional crimes that take on new life from the use of computer devices and Internet services and applications; for the second one, it is the commission of intangible crimes using technologies, such as the distribution of viruses or malicious programs through the network, attacks on websites, and software piracy. [4]. Cybercrime refers to crimes directed at both computers and/or networks and those assisted by computer technology [3]; cybercrime in the words of Lamas [8], is materialized through computer and telematic media.

Franjié [9] states that cybercrime includes crimes directed at computers and other information and communication technologies (ICTs), intrusions and denial-of-service attacks and crimes in which computers or ICTs are an integral part of the crime. This author adds that cybercrime responds to the development and economic exploitation of computers, which implies that cybercrime responds to an evolution in the use of technology, i.e., as computers were exploited, criminal ideas arose motivated by the diversity of information that these machines processed.

Therefore, Miró [10] states that cybercrime should be understood as an evolution from individual hackers to organized mafias of cybercriminals who take advantage of technological progress to increase their illicit activities and resources; being cybercrime all criminality committed in the new space.

Given the magnitude of the problem, which could cost US$10.5 trillion annually by 2025 worldwide [11] and is increasing in Latin America [1], it has been necessary to develop international instruments for its prevention, which are described in the following section.

B. International standards on cybercrime

The analysis report n°4 issued by the Office of Strategic Analysis against Crime (2021), summarizes the most important international instruments:

Within the framework of the United Nations:

a) Resolution 64/211 on the Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures, adopted by the General Assembly of the United Nations on December 21, 2009.

b) Resolution 56/121 on combating the use of information technology for criminal purposes, adopted by the United Nations General Assembly on 19 December 2001.

In the Inter-American System:

a) The Ibero-American Cooperation Agreement on Research, Assurance, and Evidence on Cybercrime Issues (2014), signed on May 28, 2014, as part of the actions promoted by the Conference of Ministers of Justice of Ibero-American countries (COMJIB); still pending the ratification by the Peruvian State.

b) The Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity (2004), approved by the General Assembly of the Organization of American States on June 8, 2004, through Resolution AG/RES. 2004 (XXXIV-0/04). It urges the member states to implement a series of recommendations in this area.

c) The Optional Protocol related to the Inter-American Convention on Mutual Assistance in Criminal Matters (1993), adopted by the Organization of American States on November 6, 1993. It entered into force on July 4, 2002. It has not been signed by Peru.

European System:

a) Directive 2016/680 of the European Parliament and the Council of Europe on the protection of natural persons regarding the processing of personal data by competent authorities for the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties, and the free movement of such data; of April 27, 2016.

b) The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007), in force since July 1, 2010, after its ratification by five member countries of the European Union, open for signature by other countries, although to date it has only been ratified at the European Union level.

c) Additional Protocol to the Convention on Cybercrime, concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (2002), adopted by the Committee of Ministers of the Council of Europe on November 7, 2002, in force since March 2006.

d) The Additional Protocol to Convention N°108 on Supervisory Authorities and International Data Flows (2001), adopted by the Council of Europe on November 8, 2001.

e) The Convention on Cybercrime or Budapest Convention (2001), approved by the Council of Europe on November 8, 2001, in force since July 2004. On February 13, 2019, by means of Legislative Resolution N°30913, the Congress of the Republic approved the accession of Peru to this Convention, which was ratified by means of Supreme Decree N°010-2019-RE, on March 9, 2019.

f) Council of Europe Convention No. 108 for the Protection of Individuals with regard to the Computerized Processing of Personal Data (1981), adopted by the Council of Europe on 8 January 1981.

C. Latin America System

TABLE I
LATIN AMERICAN LEGAL REGULATION ON CYBERCRIME

Country	Legal Regulation	Object of the regulation
Argentine	Law 26.388 of 2008	Amendment of the substantive criminal law in accordance with the Budapest Convention
	Resolution PGN No. 3743/15 dated 11/18/2015.	Designation of a magistrate of this agency as focal point, in matters related to cybercrime (Resolution PGN No. 2035/14).
Bolivia	Law 1005 dated 12/20/2017.	To prevent and punish computer crimes committed or encouraged through new technologies.
	Law No. 1768 modifying the Penal Code, dated 03/03/1997.	The Penal Code is amended by adding a chapter on computer crimes.
Brazil	LAW No. 12.737, dated 11/30/2012.	This law provides for the criminalization of computer crimes and other provisions.
Chile	Resolution N°1506, Specialized Prosecutor's Office for Money Laundering, dated 08/02/2017.	i) To be familiar with technologies and their challenges (technical and legal). ii) To have a minimum autonomous support capacity with its own tools. iii) To contribute to the system with technical standards.
	Law 19.223 dated 06/07/1993.	To typify computer crimes, the types of crimes considered, and their elements and characteristics.
	LAW 21234, dated 05/29/2020.	Amendment of Law No. 20.009, which limits the liability of credit card users for transactions made with lost, or stolen cards.
Colombia	Bill 58/2017 dated 03/06/2020.	Colombia subscribes to the Budapest Convention against cybercrime Colombia subscribes to the Budapest Convention against cybercrime.
Colombia	Law 9048 Computer Crimes, reforms and amendments to the Penal Code, of 11/2012.	New criminal offenses: identity theft, impersonation of websites, and installation or propagation of malicious software. Other crimes such as violation of correspondence and personal data, extortion, computer fraud, computer damage, and espionage.

Ecuador	Bulletin: 526 Laws, dated 08/31/2021.	Organic law reforming the comprehensive penal code to prevent and combat digital sexual violence and strengthen the fight against cybercrime.
	Agreements. 006-2021 Issue the Cybersecurity Policy, dated 06/23/2021.	The objective of this policy is to build and strengthen national capacities to guarantee the exercise of the rights and freedoms of the population and the protection of the State's legal assets in cyberspace.
Paraguay	Resolution of the State Attorney General's Office No. 4408/2011 of 2011.	To combat punishable acts committed through the use of technology that require specialized treatment, including investigation, collection, handling of evidence, and digital proof.
	Resolution No. 3459/10 establishes the criminal offenses (2010).	The criminal offenses that fall under the jurisdiction of the Specialized Unit for Computer Crimes are improper access to data, interception, preparation for improper access to data, and alteration of data.
	Law No. 3.440, dated 08/20/2008.	Amendment of several articles of the Penal Code (Law No. 1160/97), among others, those related to crimes against intellectual property.
	Law No. 5994, dated 12/20/2017.	Official accession to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature.
	Resolution No. 539 Division against computer crimes, dated 05/31/2012.	To approve the functional organic regulation of the economic and financial department of the National Police.
Perú	Law N°30096 Computer Crimes Law dated 10/21/2013.	To establishes the types of criminal offenses that can be committed by any person using information or communication technologies.
	Law N°30999, dated 08/26/2019.	Cyber Defense Law. To regulate military operations in and through cyberspace.
	Law No. 28493, dated 04/11/2005.	To regulate the sending of unsolicited commercial advertising or promotional communications by e-mail. To avoid commercial harassment.
	Law No. 27697 of 2013.	It empowers the prosecutor to intervene and control private communications and documents in exceptional cases, as amended by Law No. 30096. It adds computer crimes to the list in which the Judges will have the constitutional power.
	Legislative Decree N°1410 of 09/11/2018	To regulate and punish behaviors that represent a form of discrimination against women that have an impact on their lives and affect their rights.
	Legislative Decree N°1182, dated 07/26/2015.	To regulate the access of the specialized unit of the national police, in cases of criminal flagrancy, location, or geolocation of cell phones or electronic devices of a similar nature.
	Resolution of the Public Prosecutor's Office N° 1503-2020-MP-FN, dated 01/01/2021.	To create the Specialized Cybercrime Prosecution Unit of the Public Prosecutor's Office with national jurisdiction.
Peru	ISO/IEC 27037:2012 Ratified by AENOR, dated 12/2016.	To present the Chain of Custody (CoC) concept and establish minimum requirements to be taken into account in the identification, collection, acquisition, and preservation of potential digital evidence.
	Supreme Decree N° 010-2019-RE, dated 12/01/2019	To approve the Convention on Cybercrime, adopted in Budapest on November 23rd, 2001.
Uruguay	Law No. 20.004 dated 05/28/2014.	To approve the Ibero-American Cooperation Agreement on Research, Assurance, and Evidence on Cybercrime Issues.
Venezuela	Decree No. 3,691, dated 11/27/2018.	Regulations for the Protection of Users' Rights in the Provision of Telecommunication Services.

D. Classification of cybercrime

The Kshetri [12] classification (2013) differentiates between predatory cybercrimes and market-based cybercrimes. The former occurs in the space; the cybercriminal damages the property or the person by stealing money from the bank account or infringing intellectual property. The latter consist of the provision of services involving criminal activities, such as the sale of malicious software, the online sale of drugs, or credit card information. The difference in this classification from an economic perspective is that predatory cybercrimes do not result in the production of new goods or services, while market-based cybercrimes generate new economic value.

For this study, the classification of cybercrime developed by Miró [10] is any kind of crime where ICT is used; therefore, it happens in cyberspace. This classification is taken into consideration because it includes typologies of dangerous conducts, which put at risk various legal assets using telematic networks and other ICT systems, terminals, and services. In addition, as these typologies are integrated by ICT infrastructure, it enables a better understanding of cybercrimes so that prevention needs can be identified.

Based on the above, the objective of the systematic review is to learn about the phenomenon of cybercrime from the studies conducted by various researchers with the only purpose of understanding this phenomenon and, of course, developing new ways of prevention.

The classification proposed by Miró is developed below, since, as he states, it allows to frame all the existing typologies of criminal behavior in cyberspace, also providing differences between them.

TABLE II
CYBERCRIME CLASSIFICATION

Classification	Pure cyber-attacks	Replica cyber-attacks	Content cyber-attacks
Economic cybercrimes	Pure cyber-attacks are those that can only be possible in cyberspace. ✓ Hacking - access to a computer system or equipment without authorization of the owner. ✓ Malware - sending of viruses or other forms of file or data destruction. It can be intrusive or destructive. ✓ DoS attacks - prevent access to the system. ✓ Spam - affects the security of the system with fraudulent intent. ✓ Cybersquatting - using someone else's terminal to hack signals. ✓ Antisocial network - manipulation of social networks for fraud or any other type of crime.	Replica cyber-attacks are traditional offenses that are executed in a physical space but are carried out in a new way: by using the network. ✓ Cyber frauds - access to computer systems that give access to banking data, credit cards, pyramid or lottery scams, and even online sales in which the product is not delivered. Scam, phishing, pharming, and auction fraud, among other methods, are used. ✓ Cyber spyware – cyber spoofing (use of sniffers and other spyware). ✓ Identity theft - acquisition of another person's data to use as one's own. ✓ Spoofing uses up to five ways: Spoofing, using programs aimed at replacing the IP with another to divert the victim's information. DNS Spoofing, modifying the IP name. ARP Spoofing, sending packets from the victim to the attacking host. Web spoofing, where the user accesses a fake web page link. ✓ Corporate cyber espionage - communications are intercepted to learn trade secrets. Spyware software is installed on the computer system to send information to another system. ✓ Cyber money laundering - Internet users are used to receiving money in their accounts (mules).	Content cyber-attacks are those in which the focus of the offense is the content being communicated. Content cybercrimes can be differentiated according to: ✓ The unlawfulness of the content, such as child pornography, cyberterrorism, and encouragement of racial hatred in cyberspace. ✓ The unauthorized exploitation of content such as intellectual or industrial piracy, the discovery of trade secrets on the Internet, etc. ✓ Depending on the victim who receives the content, it can be pornography for underage people.
Social cybercrimes		✓ Cyberbullying - macro category that encompasses all behaviors in which means of communication in cyberspace are used to attack the freedom of another person. It is presented as bullying, inflicting psychological harm to the victim voluntarily and repeatedly. Cyberstalking, online harassment, in which a person is harassed, persecuted or threatened with the use of the Internet or another communication technology. ✓ Cyber sexual harassment, sexting, and online grooming - is the use of different communication tools such as Messenger, email, the oral communication system Skype or social networks such as Twitter or Facebook to attack the sexual freedom of another person. In the case of sexting, the underage person takes a nude photograph of him/herself and then sends it to another person. The problem arises when these photos are reused for more serious attacks such as cyberbullying or even sexual blackmail, known as grooming.	
Political Cybercrimes	Denial of Services (DoS) - is the use of techniques to load the resources of the target computer and cause a denial of server access to other computer systems. DoS (Cyber hacktivism) attacks - seek to damage the reputation of companies that offer services on the Internet, preventing the proper functioning of their activities. Intrusive malware.	✓ Terrorist cyber espionage ✓ Cyberwar	✓ Online hate speech ✓ Cyber-terrorism (dissemination of radical messages for terrorist purposes).

Source: Miró, 2012 [10].

II. Methodology

The methodology applied for the development of this study consisted of a systematic review study, which required an exhaustive search of articles and scientific research papers related to the topic of study. "In this regard, systematic review studies correspond to clear and systematically structured summaries of the available information aimed at answering a specific question, since they are made up of multiple articles and sources of information, representing the highest level of scientific evidence, including within their findings, important information that will contribute to the development of research on the topic under study" [13].

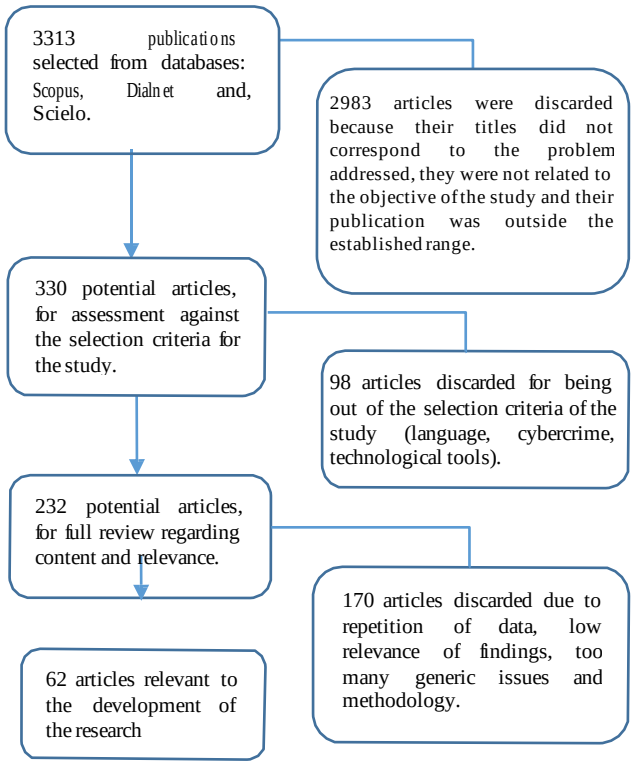
For the development of this research, a search of scientific articles published in different databases was carried out, specifically in Scopus, Dialnet and Scielo, taking into consideration keywords for the search: cybercrime, cyber delinquency, social cybercrime, economic cybercrime, political cybercrime.

Scientific articles with evidence in the study variable, graduate theses, completed and in-progress works were considered. The data collection period was carried out during January - October 2021, taking into account inclusion criteria such as publications in English and Spanish, studies oriented to the area of social sciences and engineering, and considering only scientific articles with open access published during 2009 - 2021.

Studies that address the use of technological tools as a means of committing crimes in the social sciences were also taken into consideration, which had to have concrete results. We did not consider works published in languages other than those indicated, nor those that only describe theories about technological tools or crimes.

The search, selection, and discarding path of the units of analysis used for this study is shown in Figure 1:

Figure 1: Methodological sequence in the process of search and selection of articles



Source: Search and selection diagram, adapted from Gama Zenewton & Gómez-Conesa, 2008 [14]

III. Results

A total of 62 articles that addressed problematic situations of the use of technological tools for the commission of crimes were analyzed. Table 3 shows that most of them were extracted from the Scopus database with 49 reviews, 9 articles from Dialnet, and 4 articles from Scielo:

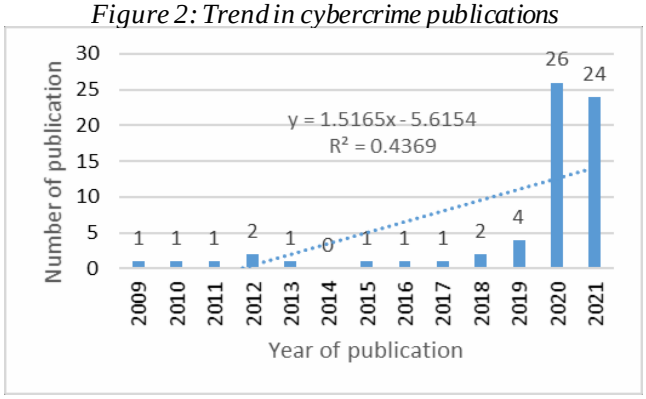
TABLE 3
ARTICLES ANALYZED BY DATABASE

Databases	N° articles	%
Dialnet	9	14%
Scielo	3	6%
Scopus	49	80%
Total	62	100%

A quantitative analysis of the frequency of articles found during 2009 - 2021 was carried out to show the trend of the need to study problems related to criminality as a consequence of the misuse of digital tools, finding a greater number of articles published during 2020 and 2021, a situation that corresponds to the beginning of social isolation as a consequence of the COVID-19 pandemic.

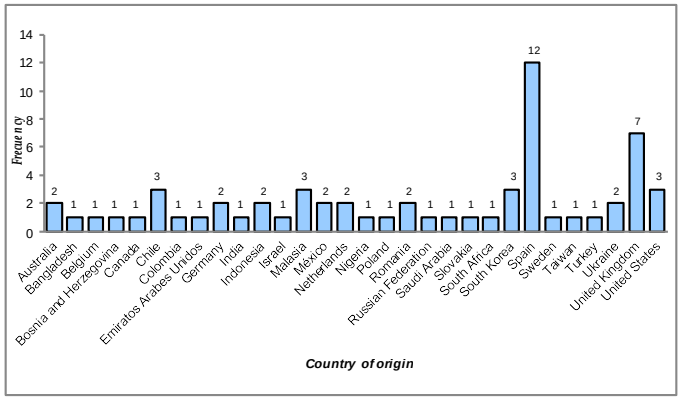
The trend analysis of the number of publications analyzed shows a positive trend over the years, as shown in Figure 2:

Figure 2: Trend in cybercrime publications



There are fewer Latin American studies (Chile 3, Colombia 1, Mexico 2), which show the need to address "cybercrime" as an issue of social necessity in the region, whose evidence will help to seek methods of prevention and action against vulnerable situations of misuse of technology in criminal acts.

Figure 3: Publications by country of origin



The figure (3) shows the number of publications by country of origin, which are part of this research; a predominant contribution of European studies is observed, especially from Spain (12) and the United Kingdom (7).

There are fewer Latin American studies (Chile 3, Colombia 1, Mexico 2), which show the need to address "cybercrime" as an issue of social necessity in the region, whose evidence will help to seek methods of prevention and action against vulnerable situations of misuse of technology in criminal acts.

The findings are described, taking into account three (3) classifications of the criminalization context: Social, Political, and Economic: [10]

TABLE IV
CRIMINALIZATION CONTEXT BY AUTHORS

Nº	Authors	Criminalization Context		
		Social	Political	conomic
1	Seung-Yeop, Mahesh K., Yong-Tae, & Julak, 2021 [3]	*	*	
2	Yuste & Pastrana, 2021[15]	*		
3	Shapira, Ayalon, Ostfel d, Farber, & Housh, 2021[16]		*	
4	Dearden, Parti, & Hawdow, 2021[17]			*
5	Sviatun, Goncharuk, Roman, Kuzmenko, & Kozych, 2021[18]		*	*
6	Sturc, Gurova, & Chernov, 2020[19]			*
7	Akinbowale, Klingelho fer, & Zerihun, 2020[5]			*
8	Srivastava, Das, Udo, & Bagchi, 2020[20]			*
9	Siddik, 2020[21]	*		
10	Onuoha Kalu, Chidi-Kalu, Achi Okidi, & Anegbemente Usiedo, 2020[22]		*	*
11	Leukfeldt & Roks, 2020[23]	*		
12	Zafer, Mehmet, & Muh ammed, 2020[24]			*
13	Szymoniak, 2021[25]			*
14	Abu Bakar & Zakaria, 2 21[26]			*
15	Găbudeanu, Brici, Mare, Cosmin Mihai, & Constantin Scheau, 2021[27]			*
16	Alzubaidi, 2021[28]		*	
17	Cascavilla, Tamburri, & Van Den, 2021[29]		*	
18	Harjinder, 2021[30]			*
19	Achim, Váidean, Borlea, & Florescu, 2021[31]			*
20	Букалерова, Остроушко, & Криез, 2021[32]	*		
21	Herrero, Torres, & Vivas, 2021[33]	*		
22	Miró Linares, 2021[34]	*		
23	Blythe & Johnson, 2021[35]			*
24	Arsawati, Darma, & Ditayani Antari, 2021[36]	*		
25	Salloum, Gaber, Vadera, & Shaalan, 2021[37]	*		
26	Stratonov, Slinko, & Slinko, 2021[38]	*		
27	Buil-Gil & Zeng, 2021[39]	*		
28	Kaddoura, Haraty, Kontar, & Alfandi, 2021[40]	*		
29	Demetis & Kietzmann, 2021[41]	*		
30	Mayer Lux & Vera Vega, 2020[42]	*		*
31	Ibañez Rodríguez, Rocha Durán, Díaz-López, Pastor-Galindo, & Gómez Mármol, 2020[43]	*		
32	Maskun, and others, 2020[44]		*	
33	De Tribolet-Hardy, Hill, & Habermeyer, 2020[45]	*		
34	Rettenberger & Leuschner, 2020[46]	*		
35	Horten & Graber, 2020[47]	*		
36	Payne, 2020[48]			*
37	Jun, 2020[49]	*		
38	Zahrah, Nurse, & Goldsmith, 2020[50]		*	
39	Mayer Lux & Oliver Calderón, 2020[51]			*
40	Drew, 2020[52]			*
41	Handaya, Yusoff, & Jantan, 2019[53]			*
42	Gassó, Mueller-Johnson, & Montiel, 2020[54]	*		
43	Gonzales Fuster & Jasmontaite, 2020[55]		*	
44	Musotto, 2020[56]			*
45	Wei-Jung, 2020[57]	*		
46	Franjié, 2020[9]	*		
47	Basuchoudhary & Searle, 2019[58]		*	*
48	Jonsoon, Fredlund, Priebe, Wadsby, & Göran Svedin, 2019[59]	*		
49	Lee, 2019[60]	*		
50	Couzigou, 2019[61]	*	*	
51	Deluca & Del Carril, 2017[62]			*
52	Ojeda Pérez, Rincón Rodríguez, Arias Florez, & Daza Martín, 2010[63]			*
53	Aguilar, 2015[64]			*

54	Miró, 2011[65]	*		
55	Miró, 2013[66]	*		
56	Pérez, 2012[67]	*		
57	González Hurtado, 2016[68]			*
58	Quintana, 2018[69]			*
59	Balcells, 2020[70]			*
60	Pons Gamon, 2018[71]			*
61	Trujano Ruiz, Dorantes Segura, & Tovilla Quesada, 2009[72]			*
62	Sanchez Madero, 2012[73]			*
Total		**28**	**11**	**29**

As shown in Table 4, the greatest criminalization context is found in "Economic" crimes with 29 cases, "Social" crimes with 28 cases, and "Political" crimes with 11 cases.

In the social context (table 3), the presence of digital tools as a means of committing crimes is evident: scripted URLs (7 references), malware (12 references), cyberspace (5 references), online games (3 references), social networks (5 references), phishing (4 references), online dating (2 references) and adult pages (4 references):

TABLE V
TECHNOLOGICAL TOOLS APPLIED TO THE COMMISSION OF CRIMES IN THE CONTEXT OF SOCIAL CRIMINALIZATION

Tool	Authors	Specific tool
Scripted URL	Seung-Yeop, 2021 [3]	o
	Siddik, 2020 [21]	o
	Miró, 2021 [34]	o
	Arsawati, 2021 [36]	o
	Demetis, 2021 [41]	o
	Mayer, 2020 [42]	o
	Gassó, 2020 [54]	o
Malware	Yuste, 2021 [15]	Malware
	Букалерова, Остроушко, & Криез, 2021[32]	Computer networks
	Herrero, 2021 [33]	Malware
	Miró, 2021 [34]	Trojans
	Kaddoura, 2021 [40]	Trojans
	Horten, 2020 [47]	Spyware
	Jun, 2020 [49]	Booter
	Franjié, 2020 [9]	Booter
	Jonsoon, 2019 [59]	Spyware
	Lee, 2019 [59]	Trojans
	Miró, 2011 [65]	Spyware
	Miró, 2013 [66]	Trojans
Cyberspace	Leukfeldt, 2020 [23]	o
	Ibañez, 2020 [43]	o
	De Tribolet-Hardy, 2020 [45]	o
	Pérez, 2012 [67]	o
	Mayer, 2020 [42]	o
Online games	Leukfeldt, 2020 [23]	o
	Herrero, 2021 [33]	o
	Jun, 2020 [49]	o
Social networks	Букалерова, Остроушко, & Криез, 2021[32]	o
	Rettenberger, 2020 [46]	o
	Jun, 2020 [49]	o
	Wei-Jung, 2020 [57]	o
	Mayer, 2020 [42]	o
Phishing	Salloum, 2021 [37]	o
	Stratonov, 2021 [38]	o
	Lee, 2019 [60]	o
	Mayer, 2020 [42]	o
Online dating	Buil-Gil, 2021 [39]	o
	Horten, 2020 [47]	o
Adult pages	Demetis, 2021 [41]	o
	Gassó, 2020 [54]	o
	Couzigou, 2019 [61]	Online chat rooms
	Mayer, 2020 [42]	Online chat rooms

o*: Not specified*

The political context (table 6) shows a different situation, emphasizing the use of malware (6 cases) as the predominant tool for committing these crimes, as well as the presence of phishing (3 references) and social networks (2 references):

TABLE VI
TECHNOLOGICAL TOOLS APPLIED TO THE COMMISSION OF CRIMES IN THE CONTEXT OF POLITICAL CRIMINALIZATION

Tool	Authors	Tool	Authors
Scripted URL	Onuoha, 2020 [22]	Social Networks	Sviatun, 2021 [18]
Malware	Shapira, 2021 [16]		Maskun, 2020 [44]
	Sviatun, 2021 [18]	Phishing	Cascavilla, 2021 [29]
	Alzubaidi, 2021 [28]		Maskun, 2020 [44]
	Cascavilla, 2021 [29]		Zahrah, 2020 [50]
	Gonzales, 2020 [55]	Online dating	Shapira, 2021 [16]
	Basuchoudhary, 2019 [58]	Adult pages	Onuoha, 2020 [22]
Cyberspace	Seung-Yeop, 2021 [3]		Couzigou, 2019 [61]
Online games	Sviatun, 2021 [18]		

Table 7 shows the tools used for the commission of economic crimes, being malware with 15 references and phishing with 9 references the most preponderant:

TABLE VII
TECHNOLOGICAL TOOLS APPLIED TO THE COMMISSION OF CRIMES IN THE CONTEXT OF ECONOMIC CRIMINALIZATION

Tool	Authors	Specific tool
Scripted URL	Akinbowale, 2020 [5]	o
	Srivastava, 2020 [20]	o
	Achim, 2021 [31]	o
	Mayer, 2020 [42]	o
	Drew, 2020[52]	o
Malware	Zafer, 2020 [24]	Booter
	Abu, 2021 [26]	Spyware, Trojan
	Găbudeanu, 2021 [27]	Malware

	Harjinder, 2021[30]	Malware
	Achim, 2021 [31]	Trojan
	Blythe, 2021 [35]	Booter
	Sviatun, 2021 [18]	Adware
	Handaya, 2020 [53]	Ransomware
	Musotto, 2020 [56]	Booter
	Basuchoudhary, 2019 [58]	Ransomware
	Deluca, 2017[62]	Trojan
	Ojeda, 2010[63]	Worms
	Aguilar, 2015[64]	Spyware, Trojan
	Mayer, 2020 [42]	Trojan
	Sanchez, 2012[73]	Trojan
Cyberspace	Onuoha, 2020 [22]	o
	Szymoniak, 2021[25]	o
	Sviatun, 2021 [18]	o
	Quintana, 2018[69]	o
	Pons Gamon, 2018[71]	o
	Sanchez, 2012[73]	o
Social networks	Sviatun, 2021 [18]	o
	Sturc, 2020[19]	o
	Onuoha, 2020 [22]	o
	González, 2016[68]	o
	Balcells, 2020[70]	o
	Trujano, 2009[72]	o
Phishing	Dearden, 2021[17]	o
	Sviatun, 2021 [18]	o
	Szymoniak, 2021[25]	o
	Găbudeanu, 2021 [27]	o
	Harjinder, 2021[30]	o
	Payne, 2020[48]	o
	González, 2016[68]	o
	Balcells, 2020[70]	o
	Trujano, 2009[72]	o
Adult pages	Akinbowale, 2020 [5]	o
	Srivastava, 2020 [20]	o
	Mayer, 2020 [42]	o
	Drew, 2020[52]	o
	González, 2016[68]	Chat sites
SIM swapping	Szymoniak, 2021[25]	o
	Achim, 2021 [31]	o
	Deluca, 2017[62]	o

o*: Not specified*

It should be taken into account that, both in contexts of social and economic criminalization, the presence of malware is preponderant, whose modes of action differ according to the context of the crime, among the most common are:

Trojans: Its name refers to what happened with the Trojan horse, because it infiltrates any device, appearing as original software and then becoming active, and it can often download new Malwares [14] [71] [66] [18]. In other words, they deceive users, who mistake it for their usual files. The danger is that when the virus is installed, the system can be remotely manipulated.

Spyware: Its name comes from its function. It is an online spy that steals information for criminal purposes. It is even used in political contexts. As Cosoi [74] says, spyware is designed to be invisible, which makes it very harmful, because the longer it goes undetected, the more damage it can cause, because it follows its victim through the use of his or her device, collecting at the same time his or her personal data.

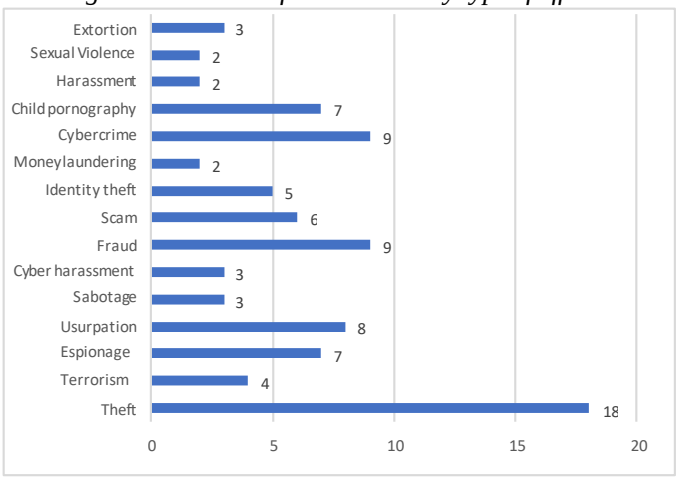
Ransomware: Software whose purpose is to gain access to systems and network resources, invading computer operations and obtaining personal information from users without their consent [75]. Ransomware acts as a means of "blackmail" by blocking access to certain files. Miró [34] notes that during the COVID-19 crisis, ransomware-type attacks against hospitals and other healthcare institutions increased. This is because cybercriminals may perceive an increased likelihood of payment due to the extraordinary circumstances created by the pandemic.[76].

Worms: They are considered among the most dangerous codes because their main characteristic is that they can self-propagate; i. e., when one of these codes is released, it does not require human intervention again to continue replicating itself in other computers [77]. As stated by Cascavilla, Tamburri & Van Den Heuvel [29], they can act as messengers in the various infected devices, while taking advantage of the information transport characteristics of the system to travel unassisted.

Booter: They are installed in devices to be controlled from a computer; they act like robots that operate in networks to organize attacks, steal data or send phishing spam [78]. According to Musotto & Wall [56], it can be hired and used to launch illegal DDoS attacks.

Adware: It is a software that acts as a recurrent advertising medium, where worms and other malware can infiltrate, in order to steal private information from the victim's PC, profile the habits of the victim user, and even use the attacked machine as a zombie for network attacks. [29] [1] According to Basuchoudhary & Searle [58] adware is annoying because it usually appears on all devices, especially smartphones and tablets, particularly when free software (freeware) or evaluation software (shareware) is installed.

Figure 4: Number of occurrences by type of offense



Authors that address the crime of Theft:[3], [17], [19], [5], [28], [29], [42], [62], [63], [65], [66], [67], [68], [70], [71], [73]; *Terrorism:* [3], [22], [50], [61]; *Espionage:* [3], [22], [24], [29], [42], [56], [58]*; Usurpation:* [15], [25], [29], [40], [42], [70], [72*; Sabotage:* [16], [18], [20]*; Cyber harassment* [21], [49], [57]*; Fraud:* [23], [24], [27], [39], [48], [51], [53], [9], [64]*; Scam:* [23], [26], [28], [46], [52], [64]*; Identity theft:* [25], [37], [55], [56], [58]*; Money laundering:* [30], [31]*; Cybercrime:* [18], [30], [31], [33], [34], [35], [38], [44], [72]*; Child Pornography:* [32], [36], [41], [43], [45], [57], [60]*; Harassment:* [46], [64]*; Sexual violence:* [54], [59]*; Extortion:* [5],[55], [56].

IV. DISCUSSIONS AND CONCLUSIONS

The frequency of cybercrime has increased significantly over the last few years, being the context of economic and social criminalization the ones with the highest incidence.

The contribution of Latin American studies on cybercrime is still limited (6 studies) compared to European and North American studies (Figure 3). However, the frequency of these criminal acts continues with alarming figures, being necessary that countries develop international standards for the prevention of cybercrime. According to the recommendations of the OAS, the commission of this type of crime is estimated at 570 million per year worldwide, and in Latin America 90 million per year.

The use of malware (Booter, Spyware, Trojan, Adware, Ransomware) is a major tool for committing crimes, whether in the political, economic, or social context. Malware is an emerging and popular threat that has been growing in the underground economies. This phenomenon occurs due to Malware-as-a-Service (MaaS) commercialization, which allows financial benefits (to criminals) to be achieved with low risk and little technical expertise. One of these popular products is ransomware, whose function is to capture data from infected systems and hold them hostage (encrypted) until a ransom is paid to the criminals. [15]

In this sense, it is essential to implement training actions within the actors in all contexts and to prevent them from becoming victims of crimes caused by this type of cyber-attacks.

Theft (18 authors), cybercrime (9 authors), and fraud (9 authors) constitute the most recurrent crimes in the review of studies conducted in this research. In the context of the COVID-19 pandemic, it is estimated that the increased anxiety caused by this increased the probability of being victims of the wide variety of cyberattacks experienced worldwide. [30]

Cybercrime prevention measures should consider that conventional malware employs standard techniques both to attack and to avoid detection, but the one that is improved is capable of hijacking the System [53]. It is essential to emphasize the training of terminal users by the various companies for which they work because, although this malware is evolving, the truth is that they always require the user of the equipment to naively open the message and perform the actions asked by the cybercriminal.

REFERENCES

[1] J. Andrew Lewis, «Los costos de la ciberdelincuencia, ¿está preparada la región?,» *MARC (Unicode/UTF-8*, pp. 101-105.

[2] UNODC, *Serie de Módulos Universitarios. Ciberdelincuencia*, Oficina de las Naciones Unidas contra la Droga y el Delito, 2020.

[3] P. Seung-Yeop, N. Mahesh K., C. Yong-Tae y L. Julak, «The Perceived Importance of Cybercrime Control among Police Officers: Implications for Combatting Industrial Espionage,» *Sustaninability*, vol. 13, nº 8, pp. 1-10, 2021.

[4] G. Sain, «La estrategia gubernamental frente al cibercrimen: La importancia de las políticas preventivas más allá de la solución penal,» de *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet*, R. A. Parada y J. D. Errecaborde, Edits., Buenos Aires, Erreius, 2018.

[5] O. Akinbowale, H. E. Klingelhofer y M. F. Zerihun, «Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature,» *Journal of Financial Crime*, 2020.

[6] Oficina de análisis estratégico contra la criminalidad, «Ciberdelincuencia: Pautas para una investigación fiscal especializada,» Ministerio Público - Fiscalía de la Nación, Lima, 2021.

[7] Y. Riega-Virú, H. L. Huamaní Chirinos y J. A. Machuca Vilchez, «Contratación electrónica y los delitos informáticos. En protección al consumidor en el Perú,» *Lex*, vol. 19, nº 28, pp. 197-236, 2021.

[8] G. L. Lamas Suárez, Cibercrimen, Bitcoins y Lavado de Activos, Lima: Litho y Arte SAC, 2019, pp. 1-151.

[9] S. Franjié, «Cybercrime is Very Dangerous Form of Criminal Behavior and Cybersecurity,» *Emerging Science Journal*, vol. 4, pp. 18-26, 2020.

[10] F. Miró Llinares, El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio, Madrid: Marcial Ponds Ediciones Juríidicas y Sociales S.A., 2012.

[11] S. Morgan, «Cybercrime Magazine,» 13 November 2020. [En línea]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[12] N. Kshetri, «Cybercrime and Cyber-security Issues Associated with China: Some Economic and Institucional Consideration,» *Electronic Commerce Research*, vol. 13, nº 1, pp. 41-69, 06 febrero 2013.

[13] B. Moreno, M. Muñoz, J. Cuellar, S. Domancic y J. Villanueva, «Revisiones Sistemáticas: definición y nociones básicas,» *Revista clínica de periodoncia, implantología y rehabilitación oral*, pp. 184-186, 2018.

[74] A. d. S. Gama Zenewton y A. Gómez-Conesa, «Factores de riesgo de caídas en ancianos: revisión sistemática,» *Revista de Saúde Pública*, vol. 42, nº 5, pp. 946-956, 2008.

[14] Z. Gama y S. Gomez-Conesa, «Avvadon ransomware: An in-depth analysis and decryption of infected systems,» *Computers & Security*, pp. 1-20, 2008.

[15] J. Yuste y S. Pastrana, «Avvadon ransomware: An in-depth analysis and decryption of infected systems,» *Computers & Security*, pp. 1-20, 2021.

[16] N. Shapira, O. Ayalon, A. Ostfeld, Y. Farber y M. Housh, «Cybersecurity in Water Sector: Stakeholders Perspective,» *Journal of Water Resources Planning and Management*, pp. 1-16, 2021.

[17] T. E. Dearden, K. Parti y J. Hawdow, «Institutional Anomie Theory and Cybercrime - Cybercrime and the American Dream, Now Available Online,» *Journal of Contemporary Criminal Justice*, pp. 1-22, 2021.

[18] O. V. Sviatun, O. V. Goncharuk, C. Roman, O. Kuzmenko y O. Kozych, «Combating cybercrime: economic and legal aspects,» *WSEAS TRANSACTIONS on ENVIRONMENT and DEVELOPMENT*, vol. 17, pp. 542-553, 2021.

[19] B. Sturc, T. Gurova y S. Chernov, «The Specifics and Patterns of Cybercrime in the Field of Payment Processing,» *International Journal of Criminology and Sociology*, vol. 9, pp. 2021-2030, 2020.

[20] S. K. Srivastava, S. Das, G. J. Udo y K. Bagchi, «Determinants of Cybercrime Originating within a Nation: A Cross-country Study,» *Journal of Global Information Technology Management*, pp. 1-27, 2020.

[21] A. B. Siddik y S. T. Rahi, «Cybercrime in social media and analysis of exist ing legal framework: Bangladesh in context,» *BiLD Law Journal*, 2020.

[22] C. Onuoha Kalu, E. Chidi-Kalu, I. A. Achi Okidi y B. Anegbemente Usiedo, «Issues on Information Systems, ICTs, Cyber-Crimes, Cyber Security, Cyber Ethics, and National Security in Nigeria: Librarians' Research,» *Library Philosophy and Practice (e-journal)*, pp. 1-19, 2020.

[23] E. R. Leukfeldt y R. A. Roks, «Cybercrimes on the Streets of the Netherlands? An Exploration of the Intersection of Cybercrimes and Street Crimes,» *Deviant Behavior*, pp. 1-13, 2020.

[24] Ö. Zafer, P. Mehmet y T. Muhammed, «Evaluation of Cybercrime Economy via MCDM and Decision Tree Approaches: The Case of Zonguldak,» *Contributions to Management Science*, pp. 521-554, 2020.

[25] S. Szymoniak, «Amelia—A new security protocol for protection against false links,» *Computer Communications*, pp. 73-81, 2021.

[26] S. N. Abu Bakar y N. H. Zakaria, «The Impact of Fear and Rational Appeal Scam Techniques on Individual Susceptibility,» *Baghdad Science Journal*, vol. 18, nº 2, 2021.

[27] L. Găbudeanu, I. Brici, C. Mare, I. Cosmin Mihai y M. Constantin Scheau, «Privacy Intrusiveness in Financial-Banking Fraud Detection,» *Risks*, pp. 1-22, 2021.

[28] A. Alzubaidi, «Cybercrime Awareness among Saudi Nationals: Dataset,» *Data in Brief*, vol. 36, pp. 1-15, 2021.

[29] G. Cascavilla, D. A. Tamburri y W.-J. Van Den Heuvel, «Cybercrime threat intelligence: A systematic multi-vocal literature review,» *Computers & Security*, pp. 1-29, 5 marzo 2021.

[30] L. Harjinder, «Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic,» *Kent Academic Repository*, nº 1-22, 2021.

[31] M. V. Achim, V. L. Váidean, S. N. Borlea y D. R. Florescu, «The Impact of the Development of Society on Economic and Financial Crime. Case Study for European Union Member States,» *Risks*, pp. 1-20, 2021.

[32] I. A. Букалерова, A. B. Остроушко y O. Криез, «Crimes against the information security of minors committed through information and telecommunication networks (including the Internet),» *Vestnik Sankt-Peterburgskogo Universiteta. Pravo*, vol. 12, pp. 17-35, 2021.

[33] J. Herrero, A. Torres y P. Vivas, «Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization,» *International Journal of Environmental Research and Public Health*, vol. 18, pp. 1-11, 2021.

[34] F. Miró Llinares, «Crimen, cibercrimen y COVID-19:,» *Revista de los Estudios de Derecho y Ciencia Política*, nº 32, pp. 1 - 17, 03 2021.

[35] J. M. Blythe y S. D. Johnson, «A systematic review of crime facilitated by consumer Internet of Things,» *UCL Jill Dando Institute of Security and Crime Science*, vol. 34, pp. 97-125, 2021.

[36] N. J. Arsawati, M. W. Darma y P. E. Ditayani Antari, «A Criminological Outlook of Cyber Crimes in Sexual Violence Against Children in Indonesian Laws,» *International Journal of Criminology and Sociology*, vol. 10, pp. 219-233, 2021.

[37] S. Salloum, T. Gaber, S. Vadera y K. Shaalan, «Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey,» *Procedia CIRP*, vol. 189, pp. 19-28, 2021.

[38] V. Stratonov, D. Slinko y S. Slinko, «Some types of computer and cybercrime in Ukraine,» *Access to Justice in Eastern Europe*, vol. 4, pp. 191-197, 2021.

[39] D. Buil-Gil y Y. Zeng, «Meeting you was a fake: Investigating the increase in romance fraud during COVID-19,» *Journal of Financial Crime*, pp. 1-17, 2021.

[40] S. Kaddoura, R. A. Haraty, K. A. Kontar y O. Alfandi, «A Parallelized Database Damage Assessment Approach after Cyberattack for Healthcare Systems,» *Future internet*, vol. 13, pp. 1-18, 2021.

[41] D. S. Demetis y J. Kietzmann, «Online sexual abuse of adolescents by a perpetrator met online: a cross-sectional study,» *Child and Adolescent Psychiatry and Mental Health*, vol. 13, pp. 1-10, 2019.

[42] L. Mayer Lux y J. Vera Vega, «The crime of cyber espionage: Definition and delimitation,» *Journal of the Association for*, vol. 22, nº 9, pp. 5-40, 2021.

[43] J. Ibañez Rodríguez, S. Rocha Durán, D. Díaz-López, J. Pastor-Galindo y F. Gómez Mármol, «C3-Sex: A Conversational Agent to Detect Online Sex Offenders,» *Electronics*, vol. 9, nº 1779, pp. 1-23, 2020.

[44] Maskun, Achmad, Naswar, H. Assidiq, A. Syafira, M. Napang y M. Hendrapati, «Qualifying Cyber Crime as a Crime of Aggression in International Law,» *Journal of East Asia and International Law*, vol. 13, pp. 397-418, 2020.

[45] F. de Tribolet-Hardy, A. Hill y E. Habermeyer, «Webcam child sexual abuse,» *Forensische Psychiatrie, Psychologie, Kriminologie*, vol. 14, pp. 259-269, 2020.

[46] M. Rettenberger y F. Leuschner, «Cyberkriminalität im Kontext von Partnerschaft, Sexualität und Peerbeziehungen: Zur Cyberkriminologie des digitalen sozialen Nahraums,» *Forensische Psychiatrie, Psychologie, Kriminologie*, vol. 14, pp. 242-250, 2020.

[47] B. Horten y M. Graber, «Cybercrime: Overview of current and future manifestations,» *Forensische Psychiatrie, Psychologie, Kriminologie*, vol. 14, pp. 233-241, 2020.

[48] B. K. Payne, «Criminals Work from Home during Pandemics Too: a

Public Health Approach to Respond to Fraud and Crimes against those 50 and above,» *American Journal of Criminal Justice*, pp. 563-577, 2020.

[49] W. Jun, «A Study on the Cause Analysis of Cyberbullying in Korean Adolescents,» *International Journal of Environmental Research and Public Health*, vol. 17, nº 4, pp. 1-17, 2020.

[50] F. Zahrah, J. R. Nurse y M. Goldsmith, «#ISIS vs #ActionCountersTerrorism: A Computational Analysis of Extremist and Counter-extremist Twitter Narratives,» *Proceedings - 5th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2020*, pp. 438-447, 2020.

[51] L. Mayer Lux y G. Oliver Calderón, «El delito de fraude informático: Concepto y delimitación,» *Revista Chilena de Derecho y Tecnología*, vol. 9, nº 1, pp. 151-184, 2020.

[52] J. Drew, «A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies,» *Journal of Criminological Research, Policy and Practice*, pp. 17-33, 2020.

[53] W. B. Handaya, M. N. Yusoff y A. Jantan, «Machine learning approach for detection of fileless cryptocurrency mining malware,» *Journal of Physics: Conference Series*, vol. 1450, 2019.

[54] A. M. Gassó, K. Mueller-Johnson y I. Montiel, «Sexting, Online Sexual Victimization, and Psychopathology Correlates by Sex: Depression, Anxiety, and Global Psychopathology,» *International Journal of Environmental Research and Public Health*, vol. 17, 2020.

[55] G. Gonzales Fuster y L. Jasmontaite, «Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights,» de *The Ethics of Cybersecurity*, vol. 21, Brussels, Springer Open, 2020, pp. 97-115.

[56] R. Musotto y D. S. Wall, «More Amazon than Mafia: Analysing a DDoS stresser service as organised cybercrime,» Trends in Organized Crime, vol. 25, pp. 173-191, 04 November 2020

[57] C. Wei-Jung, «Cyberstalking and law enforcement,» *Procedia Computer Science*, pp. 1188-1194, 2020.

[58] A. Basuchoudhary y N. Searle, «Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets,» *Computers & Security*, vol. 87, pp. 1-13, 2019.

[59] L. Jonsoon, C. Fredlund, G. Priebe, M. Wadsby y C. Göran Svedin, «On line sexual abuse of adolescents by a perpetrator met online: a cross - sectional study,» *Child Adolesc Psychiatry Ment Health*, 24 agosto 2019.

[60] J. Lee, «Child Pornography Websites on the Darknet,» *International Journal of Recent Technology and Engineering*, pp. 48-54, 2019.

[61] I. Couzigou, «The Criminalization of Online Terrorism Preparatory Acts Under International Law,» 2019.

[62] S. Deluca y E. Del Carril, «Cooperación internacional en materia penal en el mercosur: El cibercrimen,» vol. 5, nº 10, pp. 13-28, 2017.

[63] J. E. Ojeda Pérez, F. Rincón Rodríguez, M. E. Arias Florez y L. A. Daza Martín, «Computer crime and current legislation in Colombia,» *Cuadernos de Contabilidad*, pp. 41-66, 2010.

[64] M. M. Aguilar Cárceles, «Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido,» *Revista Criminal*, vol. 57, nº 1, pp. 121-135, 2015.

[65] F. Miró Llinares, «La oportunidad criminal en el ciberespacio,» *Revista electrónica de ciencia penal y criminología*, pp. 07:01 - 07:55, 2011.

[66] F. Miró Linares, «La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio,» *Revista española de investigación criminológica*, vol. 5, nº 11, pp. 1-35, 2013.

[67] J. Pérez Gil, «Recensión del libro de Fernando Miró Linares, El Cibercrimen Fenomenología y criminología de la delincuencia en el ciberespacio,» *Revista electrónica de ciencia penal y criminología*, nº 15-r2,, pp. r2:1-r2:05, 2013.

[68] J. A. González Hurtado, «La seguridad en los sistemas de información como un bien jurídico de carácter autónomo. Perspectiva europea y española,» *Revista penal México*, nº 9, pp. 59-76, Mexico 2016.

[69] Y. Quintana, «Ciberseguridad, una cuestión de Estados,» *Política exterior*, vol. 32, nº 185, pp. 50-57, 2018.

[70] M. Balcells, «Una nueva edición del congreso IDP en formato virtual dedicada al cibercrimen,» *Revista de los Estudios de Derecho y Ciencia Política*, nº 31, octubre 2020.

[71] V. Pons Gamon, *Ciberterrorismo: Amenaza a la seguridad. Respuesta Operativa y Legislativa, Nacional e internacional*, 2018, pp. 1-562

[72] P. Trujano Ruiz, J. Dorantes Segura y V. Tovilla Quesada, «Violencia en Internet: Nuevas víctimas, nuevos retos,» *Liberabit*, vol. 15, nº 1, pp. 7 - 19, 2009.

[73] G. Sánchez Madero, «Ciberespacio y el Crimen Organizado. Los nuevos desafíos del siglo XXI,» *Ciencia Política y Administración Pública,*, vol. 10, nº 16, pp. 71-87, 2012.

[74] E. Cosoi P., «Scielo,» *Revista chilena de Pediatría*, vol. 74, nº 4, pp. 432-433, Julio 2003.

[75] R. R. Guevara, «Detección y clasificación de Malware con el Sistema de Análisis de Malware Cuckoo,» Universidad Internacional de La Rioja, Madrid, 2018.

[76] H. Lallie, L. A. Shepherd, . J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple y X. Bellekens, «Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic,» Kent Academic Repository, pp. 1 - 22, 2021.

[77] J. A. González, H. P. Meana y P. G. López, «Gusanos Informáticos,» Comunicaciones Libres, pp. 85-87, 2015.

[78] A. J. Omaña-Butrón, R. Galván-Guerra, A. Leines-Martínez, A. Ramírez-Díaz y J. E. Velázquez-Velázquez, «Implementacion de Controladores por Modos Deslizantes en un Convertidor Boost,» *Boletín Científico de Ciencias Básicas e Ingenierías de ICBI*, vol. 8, nº 15, pp. 82-91, 07 Mayo 2020.