CYBERCRIME IN EUROPA

Gheorghe (Nițu) Maria (author for correspondence), Romania, nitumaria2@gmail.com
Dumitrescu Mihaela-Sorina, Bucharest University of Economic Studies, Romania, sorina.dumitrescu15@yahoo,com
Florea Oana, Bucharest University of Economic Studies, Romania, oana.stefaneascu@stud.ase.ro

We suggest you to cite this article as:
Gheorghe (Nițu), M., Dumitrescu, M.S., Florea, O. Cybercrime in Europa. *Junior Scientific Researcher*, Vol VII, No. 2, pp. 39-48.

Abstract

T*he latest technological advance has generated a multitude of possibilities for states, companies, citizens, as a major step in improving the quality of life and the way of doing business, but it has created the opportunity for criminals to carry out illegal activities, via the internet. Thus, the phenomenon of cybercrime has spread globally, manifesting itself in the form of extremely complex attacks, crimes in the area of advanced technology that are aimed at computer systems as a result of the global use of the Internet and the enormous volume of information.*
The European Union focuses on cybercrime and, through the Directives, it gives legal space to prevent and combat it, by punishing the attackers, who manage to commit these attacks and adapt continuously. Thus, in order to fight cybercrime, companies, the European Union are actively involved in conducting studies and research designed to help combat and eradicate these crimes. The purpose of this paper is to present the phenomenon of cybercrime in the European Union by exposing the most representative definitions, types, modalities of action and the effects they cause, the measures that are taken at European level through the Directives, and also research on the impact of cybercrime.

Keywords*: Cybercrime, European Union, Directives, Specops, Special Eurobarometer 499, Microsoft Digital Defense Report*

JEL Classification*:* K24

Introduction

Technological developments, computers, the Internet, etc. have had a major impact on all aspects of human life, revolutionizing and changing the way we communicate, make payments, shop, and even spend our free time (Holt and Bossler, 2018).

One of the characteristics of today's world is cyberspace which has created a new way of living and doing activities, connecting people from different parts of the globe, both from developed and developing countries. However, the opportunities generated by technology were followed, in parallel by the negative effects, offering the possibility to the perpetrators to commit crimes against users/citizens, companies, states. The attackers specialized and became better and better prepared, managing to act anonymously and create major damage to the intended victim.

As a result, European authorities, companies have turned their attention and focused their resources on studying cybercrime and its effects, by collecting data and conducting studies to help minimize its impact. The European institutions, together with the member states, are vigilant about the changes that appear and, through the Directives, create the legislative dimensions in order to prevent and fight cybercrime, but also of the possible new types of crimes.

Background

Cybercrime represents a type of crime carried out in the online word/internet (Oxford, 2009), a criminal activity executed in order to access, manipulate or transmit information/data using a computer (Merriam-Webster, 2017). Online crime is called cybercrime and is committed by individuals who have experience and high knowledge (Holt, Bossler and Seigfried-Spellar, 2018) in this field. Thus, this concept designates a wide and varied range of crimes, such as and illicit behaviors that certain groups or individuals commit within the computer network, against computers and other types of devices or types of traditional crimes and activities that pursue certain individuals, through technology or the Internet (Donalds, Osei-Bryson, 2019).

According to Interpol, cybersecurity does not have a generally valid definition, but this illegal action involves complex attacks and crimes in the advanced technological area aimed at computer systems, computer data, providers, services, including: fraud, illegal access, illegal interception of information, data, data interference, etc. (Interpol, 2021, p.8, 9). According to Europol, the nature of cybercrime is borderless, making it extremely difficult for authorities to conduct criminal investigations (Europol, 2016), but also the alarming increase in trends in the use of technology through which illegal actions are committed (United Nations, 2005). In 2001, the European Council introduced cybercrime as an illegal activity with or against a computer.

Cybercrime is extremely complex and brings together a large number of crimes such as: Malware, online fraud, cyber bullying, spamming, hacking, cyber threats, online banking fraud, payments, etc. (Reep-van den Bergh & Junger, 2018). According to a study by E&Y, is cybersecurity about more than protection? - EY Global Information Security Survey 2018-2019, in the top 10 on cyber threats importing companies we find first place phishing 22%, followed by malware 20%, cyberattacks - to disrupt 13% and to steal money 12%, fraud 10 %, on the last place ranking espionage with 2% (EY, 2019, p. 9).

Thus, cybercrime is an illegal act that is committed by resorting to "computer, network or hardware device" (Gordon & Ford, 2006, p. 14), in the same directive being described cybercrime by the Council of Europe in 2001, a crime that is committed via computer or network. It can be divided into 3 categories: crimes characteristic of the Internet, online fraud or forgery and online illicit content (European Commission, 2019, p.3).

In their research, Ngo and Jaishankar (2017) focused on the 5 dimensions of the phenomenon from the perspective of cyber criminology: the presentation and ranking of cybercrime, dominance, trends and nature, promotion, research of good practice to prevent and combat cybercrime and shifting attention to privacy issues (Ngo & Jaishankar, 2017, pp. 2-6). Cybercrime is similar to crime traditionally made as a result of the fact that they “take multiple forms with expressive and/or instrumental value to the offender” (Leukfeldt, Holt, 2021, p. 2). For example, actions such as cyberbullying or

online harassment give the offender the same kind of power as if they were actually doing so (Leukfeldt, Holt, 2021; Holt & Bossler, 2015; Patchin & Hinduja, 2013), and phishing, as well as Online fraud involves collecting information or personal data for use in order to obtain financial benefits (Leukfeldt, Holt, 2021). A problematic element of cybercrime is the complexity of this process which can include a variety of crimes, which can be assessed both from an economic perspective and from an ideological or even revenge perspective (Leukfeldt,et al. 2017).

From a classification perspective, cybercrime can take place against certain groups of people or individuals, users or computer networks (Wagen and Pieters, 2020; Ho & Luong, 2022, p.2) or cyber-violence, cyber-deceptions, cyberpornography, cyber-trespass, etc. (Wall, 2001; Ho & Luong, 2022, p.2). Ho and Luong (2022) also classified cybercrime into 2 categories: "cyber-dependent crime (Malware, hacking, denial of service attacks) and cyber-enable crime (online shopping fraud, identity thief, phishing)" (Ho & Luong (2022) classified Luong, 2022, p.2).

Therefore, cybercrime is the illegal operation committed by criminals who use technology, through smartphones, computers, tablets, etc. (Perwej et all, 2021), as well as theft, destruction, misuse, seizure of information, unauthorized modification of their equipment. , services, etc. (Perwej et all, 2021). However, cybercrime encompasses both traditionally committed crimes that have benefited from the benefits of information and communication technology (ICT) and the creation of computers, tablets, smartphones, and the Internet (Ho & Luong, 2022).

Cybercrime is on the rise, impacting societies, governments, and companies with detrimental effects on citizens and a detrimental impact on economies (Donalds, Osei-Bryson, 2019).

In the document made for the 10th edition of the United Nations Congress on the Prevention of Crime and the Treatment of Offenders, there is a distinction between cybercrime (United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, p.5, Broadhead, 2018, pp. 1182):

- *"computer crime (narrow sense): represent any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them";*
- *"computer-related crime (broader sense): represent any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network".*

At the European Union level, guidelines have been drawn up for computer-based crime, a tool in the process of preventing and combating cybercrime according to the Council of Europe Convention on Cybercrime (Budapest 23.11.2001), and The Budapest Convention on Cybercrime 13.07.2020. Thus, The Budapest Convention on Cybercrime from 13.07.2020 establishes aspects such as: effective international cooperation, tools, procedural legal levers to investigate cybercrime and secure electronic elements that prove the connection with crimes, accusations of conduct aimed at illegal access data, etc., being considered one of the most important international agreements on cybercrime (Council of Europe, 2020, p.4). At the same time, it requires States to criminalize computer-based crimes under Articles 2 to 12, in the domestic law of each Member State, their authorities and their powers to investigate all crimes (according to Table 1).

Table nr. 1

Substantive criminal law: offences	Procedural law to secure evidence and investigate	International cooperation
Art. 2 – Illegal access Art. 3 – Illegal interception Art. 4 – Data interference Art. 5 – System interference Art. 6 – Misuse of devices Art. 7 – Computer-related forgery Art. 8 – Computer-related fraud Art. 9 – Child pornography Art. 10 – IPR offences Art. 11 – Attempt, aiding, abetting Art. 12 – Corporate liability	Art. 14 – Scope of procedural provisions Art. 15 – Conditions and safeguards Art. 16 – Expedited preservation Art. 17 – Expedited preservation and partial disclosure of traffic data Art. 18 – Production order Art. 19 – Search and seizure Art. 20 – Real-time collection traffic data Art. 21 – Interception of content data	Art. 23 – General principles Art. 24 – Extradition Art. 25 – General rules Art. 26 – Spontaneous information Art. 27 – MLA in absence of treaty Art. 28 – Confidentiality Art. 29 – Expedited preservation Art. 30 – Partial disclosure traffic data Art. 31 – MLA accessing data Art. 32 – Transborder access Art. 33 – MLA collection traffic data Art. 34 – MLA interception content Art. 35 – 24/7 point of contact

Sources: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac, p. 5

Methods

The main purpose of the articles is to present the phenomenon of cybercrime in the European Union, using the method of qualitative research. Thus, first of all, we reviewed the concept of cybercrime by presenting the most representative definitions, types and methods of action, in order to understand this type of crime and the effects it can have both at the macro (country) level, as well as micro level, within companies or on citizens. Secondly, we presented some studies on cybercrime conducted by:

- European Commission through Special Eurobarometer 499 which measures the perception, experiences and attitudes of citizens regarding cybercrime;
- Specops Software that performs a ranking of countries exposed to cybercrime versus countries that cope with this crime;
- Microsoft, which, based on the data collected, presented the most exposed fields of activity, but also countries in cybercrime;
- Allianz Global Corporate Specialty on the highest business risks in 2022.

Last but not least, we have briefly presented the actions and measures of prevention and control taken at European level in this direction, so that the impact is as small as possible.

Therefore, this paper shows the magnitude of the cybercrime phenomenon and the impact it can have in the current context, but also the speed with which criminals manage to identify new, illegal methods of attack, creating significant damage, but also a state of anxiety as a result that they act under the umbrella of anonymity and even from a distance.

Results and discussions, including research limits and advantages

The European Union has about 600 cybersecurity centers and more than 60,000 cybersecurity companies, and in terms of the Global Security Index, the countries of the

European Union rank on "18 of the 20 places" (European Council, Council of the European Union, 2022), demonstrating the importance of this issue, but also the measures taken to combat and prevent cybercrime, by implementing laws and supporting operational cooperation, because this type of crime does not take into account borders. (European Council, Council of the European Union, 2020).

According to a study conducted by Specops Software experts for 2019, below you can see the ranking of countries exposed to cybercrime versus countries that are more secure in this regard, researching "the percentage of cloud provider attacks on Azure and the monthly percentage of machines that encountered cryptocurrency mining, malware and ransomware ”(SPECOPS, 2020).

Tabel No. 1
The most cyber insecure countries

The most cyber insecure countries
1. Netherlands
2. Bulgaria
3. Belarus
4. Ukraine
5. Bosnia and Herzegovina
6. Lithuania
7. Romania
8. France
9. Hungary
10. Croatia

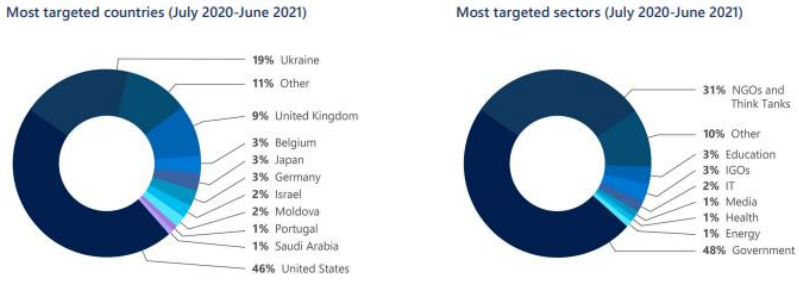
Table No. 2
The most cyber secure countries

The most cyber secure countries
1. Ireland
2. Norway
3. Denmark
4. Switzerland
5. Iceland
6. Sweden
7. Belgium
8. Luxembourg
9. Czechia
10. Finland

Source: SPECOPS, 2020
https://specopssoft.com/blog/european-countries-cyber-crime/

Thus, it can be seen that in table 1 are the EU countries that are not very safe for citizens in terms of cybercrime, among which we list the Netherlands, France, Ukraine, Romania, Bulgaria, etc., compared to table 2 which lists 10 cyber secure countries, as follows Ireland, Denmark, Norway, Switzerland, etc. Global events (Covid-19 pandemic, teleworking) have led to a rapid and significant increase in cybercrime by updating and refining methods of attacking cybercriminals that harm not only companies but also citizens and states The Microsoft Digital Defense Report, based on the data collected, includes an x-ray of the current cyber situation, but also the main indicators in the early detection and anticipation of future actions of attackers, and the 2020 report mentions common techniques (malware, VPN, credential harvesting, ECT) but also the goals (disruption or destruction, espionage) which are dominant among the main cyber representatives in the nation states (Microsoft, 2021). In the Figure below (Fig 1), most targeted countries (July 2020-June 2021), we find EU countries, such as Ukraine which has a very high percentage of 19%, second after the United States (46%), Belgium and Germany 3%, Moldova 2% and Portugal 1%, suggesting a high level of cybercrime attention on the European region.

Figure No. 1 Most targeted countries and Most targeted sectors (July 2020-June 2021)

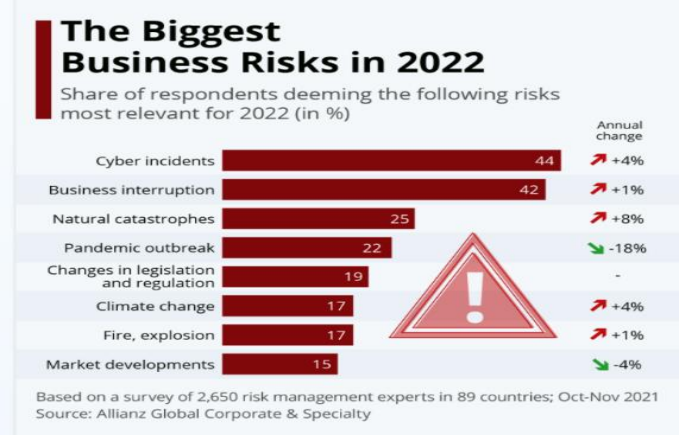


Sources:Microsoft, 2021 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFli#page=47, p. 5.

The same report also classified the most target sectors for the same period (July 2020-June 2021), with Government 48% followed by NGOs and Think Tanks 31%, education 3%, IT 2%, Health and Energy 1% (Microsoft, 2021, p. 53).

The survey conducted by Allianz Global Corporate Specialty suggests that more than 40% of experts surveyed consider cyber crime to be the main business risk in 2022, followed by 42% business interruption, 25% natural catastrophes and 22% pandemic outbreak.

Figure No. 2 The Biggest Risks in 2022



Sources : https://www.statista.com/chart/26631/most-relevant-business-risks-in-2022/

The phenomenon of cybercrime is also present in the case of citizens, individuals, who feel its effects. According to Special Eurobarometer 499, which examines Europeans' attitudes, perceptions and experiences regarding cybercrime in 2019, they report that 52% of them believe they have enough information about cybercrime compared to 46% in 2017, but from the perspective of trust and capacity to protect against this crime the percentage is decreasing in 2019, only 59% as opposed to 71% in 2017 (Directorate-General for Communication, 2020). This survey was conducted between October 8-22, 2019, at EU level, and is divided into 4 chapters (1. Use of the Internet, devices and activities carried out by citizens, 2. Attention to the elements of online security and any changes of the confidentiality and security, 3. The degree of information of the individuals regarding the risks, their experiences and the possible measures taken

regarding the protection of children, 4. Awareness regarding the reporting of possible crimes/illegal behaviors online) participating a number of 27,607 respondents (Directorate- General for Communication, 2020).

Thus, at the level of the European Union, as a result of the increased use of the Internet and various devices for activities such as: online shopping, online payments, teleworking, etc., but also the Covid-19 pandemic has increased the potential and risks of cybercrime, because criminals are very vigilant and manage to adapt their methods of attack to current vulnerabilities and achievements, especially since it is expected that at European level, by 2024, 22.3 million devices will be connected to IoT (European Council, Council of the European Union, 2022).

The European Union is actively involved in the process of combating and preventing cybercrime through continuous and adapted measures and actions, issuing directives:

- The convention on the Prevention of Terrorism in 2005;
- The Lanzarote Convention in 2007;
- Directive 2011/93 / EU of the European Parliament and of the Council on combating the sexual exploitation of children and child pornography;
- Directive 2013/40 / EU of the European Parliament and of the Council on attacks against information systems by which Member States are required to introduce more severe criminal sanctions and to strengthen their national laws;
- Proposals for Regulation and Directive facilitating cross-border access to electronic evidence for criminal investigation in 2018 and funding projects such as SIRIUS and EVIDENCE project;
- EU Directive 2019/713 of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment.

The European Cybercrime Center (EC3) has also been set up, which focuses on payment fraud, child sexual exploitation and cyber-dependent crime, as well as the Cybercrime Program Office (C-PROC) N based in Bucharest, Romania. facing threats from cybercrime.

Conclusions

The development of technology has been a major step in improving lives, but it has provided new opportunities for criminals to commit illegal actions, especially through the Internet, which has allowed them to operate anonymously and even remotely.

The phenomenon of cybercrime has become more and more present in the lives of citizens, Europeans, but also in companies and states, due to its dynamic nature and in full expansion, managing to adapt to new realities and especially to the widespread expansion of The Internet and the large volume of information, its implementation in most operations performed at the level of individual, enterprise and countries. It is difficult to issue a generally valid and applicable definition of this type of crime, which is unpredictable and can create major damage in all areas of activity (health, education, finance, business, transportation, public administration, etc.). Cybercrime brings together a considerable number of crimes (for example: phishing, malware, online fraud, hacking, cyber bullying) which can have major repercussions on the intended target.

At the European Union level, various studies have been conducted on the impact of cybercrime on countries, companies and citizens. For example, Specops Software has

made a ranking of the most insecure countries versus those that are prepared for these attacks, Allianz Global Corporate Specialty presented that cybercrime ranks first in terms of business risks in 2022, Microsoft made a ranking of areas of activity prone to cybercrime, and the Special Eurobarometer 499 investigated the experiences of Europeans on this crime.

At the same time, the European Union, through the directives, creates a clear space for regulation and counter-attack on cybercrime, identifying vulnerabilities and classifying crimes committed in the online space, so that there is a clear, legal framework for sanctioning criminals.

Efforts to prevent and combat cybercrime are collective, it can be seen that large companies are actively involved in researching this phenomenon and trying to reduce the negative effects, and European institutions are constantly updating and adapting legislation to new types of crime, but also debates constructive in order to identify the best solutions for the actors involved.

Although the forces are focused on combating cybercrime, the measures taken and the actions taken have not completely eradicated it, being a difficult and long process due to the global use of the Internet and the enormous volume of information, but also the capacity of criminals to adapt their methods of attack, especially since they are specialized and organized.

Bibliography

1. Allianz Global Corporate & Specialty. (2022) The Biggest Business Risks in 2022 [Online] Available from: https://www.statista.com/chart/26631/most-relevant-business-risks-in-2022/ [Accessed: 1st of March, 2022].
2. BRADBURY, I., BOYLE, J. and MORSE, A. (2002) Scientific Principles for Physical Geographers. Harlow: Prentice Hall.
3. BROADHEAD, S. (2018) A contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and development, Computer Law & Security review, 43, p. 1180-1196, Available from: https://doi.org/10.1016/j.clsr.2018.08.005 [Accessed: February 10th , 2022]
4. CARIN M. M. REEP-VAN DEN BERGH, C. M.M., JUNGER, M. (2018) Victims of cybercrime in Europe: a review of victim survey, 2018, Crime Science, Springer Open, 7 (5), p. 1-15, Available from: https://doi.org/10.1186/s40163-018-0079-3 [Accessed: 30th January, 2022]
5. Commission. (2018) Proposals for Regulation and Directive faciliting cross-border access to electronic evidence for criminal investigation Available from: https://ec.europa.eu/home-affairs/cybercrime/e-evidence_en [Accessed: 1st of March, 2022]
6. Council of Europe. (2020) Cybercrime Convention Committee (T-CY). The Budapest Convention on Cybercrime : benefits and impact in practice [Online] Available from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac [Accessed: March the 5th , 2022].
7. Directorate-General for Communication. (2020) Barometrul special 499: Atitudinea europenilor fata de securitatea cibernetica (Criminalitatea cibernetica) [Online] Available from: https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=ro [Accessed: March the 5th, 2022].
8. DONALDS, C., OSEI-BRYSON, K-M. (2019), Toward a cybercrime classification ontology: A knowledge-based approach, Computers in Human Behavior,92, P. 403–418, Available from; https://doi.org/10.1016/j.chb.2018.11.039 [Accessed: 30th January, 2022]
9. European Comission. (2019) Europeans" attitudes toward cyber security [Online] Available from: https://op.europa.eu/en/publication-detail/-/publication/468848fa-49bb-11ea-8aa5-01aa75ed71a1[Accessed: March the 5th,2022].

10. European Council, Council of the European Union. (2020) Cybersecurity: how the EU tackles cyber threats [Online] Available from: https://www.consilium.europa.eu/en/policies/cybersecurity/ [Accessed: March 25, 2022].
11. European Parliament, Council. (2011) Directive 2011/93/EU on combating the sexual exploitation of children and child pomography [Online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093 [Accessed: March 25, 2022]
12. European Parliament, Council. (2013). Directive 2013/40/EU on attacks against information systems [Online] Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040 [Accessed: March 25, 2022]
13. European Parliament, Council. (2019). Directive EU 2019/713 on combating fraud and counterfeiting of non-cash means of payment [Online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.ENG [Accessed: March 25, 2022]
14. Europol. (2016) Cybercrime presents a major challenge for law enforcement [Online] Available from: https://www.europol.europa.eu/media-press/newsroom/news/c ybercrime-presents-major-challenge-for-law-enforcement [Accessed: March 25, 2022].
15. EY. (2019) Global Information Security Survey 2018-2019. [Online] Available from: https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf [Accessed: 15th March, 2022].
16. GORDON, S., & FORD, R. (2006). On the definition and classification of cyber crime. Journal of Computer Virology, 2, p. 13-20, Available from: https://link.springer.com/content/pdf/10.1007/s43545-021-00305-4.pdf [Accessed: 30th January, 2022]
17. HOLT, T. J., & BOSSLER, A. M. (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses. London: Routledge. [Online] Available from: https://click.endnote.com/viewer?doi=10.4324%2F9781315775944&token=WzMyODc1MDEsIjEwLjQzMjQvOTc4MTMxNTc3NTk0NCJd.ZCX8illHAqmJjlZRPQ6Iezy8j98 [Accessed: February 25, 2022]
18. Interpol. (2021) National Cybercrime Strategy. Guidebook. Available from: https://www.interpol.int/content/download/16455/file/National%20Cybercrime%20Strategy%20Guidebook.pdf [Accessed: March 20, 2022]
19. LEUKFELDT, E., R., HOLT, T. J. (2021), Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals, Computers in Human Behavior, 126 ,p 1-9. Available from: https://doi.org/10.1016/j.chb.2021.106979 [Accessed: February 10th, 2022]
20. LEUKFELDT, E.R., LAVORGNA, A., KLEEMANS. E.R. (2017) Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime, Eur J Crim Policy Res, 23, p.287–300. Available From: 10.1007/s10610-016-9332-z [Accessed: 30th January, 2022]
21. Merrian Webster. [Online] Available from: https://www.merriam-webster.com/dictionary/cybercrime#legalDictionary [Accessed: February 10th, 2022].
22. Microsoft. (2021) Digital Defense Report [Online] Available from: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi#page=47 [Accessed: March 20, 2022]
23. NGO, F., JAISHANKAR, K. (2017) Commemorating a decade in existence of the international journal of cyber criminology: a research agenda to advance the scholarship on cyber crime. Int J Cyber Criminol 11(1), p. 1–9, Available from: https://www.researchgate.net/publication/316860618_Commemorating_a_Decade_in_Existence_of_the_International_Journal_of_Cyber_Criminology_A_Research_Agenda_to_Advance_the_Scholarship_on_Cyber_Crime/link/591495cd0f7e9b70f49c22a8/download [Accessed: February 10th, 2022]
24. Oxford Reference (2009) [Online] Available from: https://www.oxfordreference.com/view/10.1093/acref/9780199551248.001.0001/acref-9780199551248-e-1000 [Accessed: February 10th, 2022].
25. PATCHIN, J. W., & HINDUJA, S. (2013). Cyberbullying among adolescents: Implications for empirical research. Journal of Adolescent Health, 53(4), p. 431–432. Available from: https://www.researchgate.net/publication/256927872_Cyberbullying_Among_Adolescents_Implications_for_Empirical_Research [Accessed: February 10th, 2022]

26. PERWEJ, Y., ABBAS, S.O., DIXIT, J.P., AKHTAR, N., JAISWAL, A.K. (2021) A Systematic Literature Review on the Cyber Security. International Journal of scientific research and management, International Journal of scientific research and management, 2021, 9 (12), p.669-710. Available from: ff10.18535/ijsrm/v9i12.ec04ff. ffhal-03509116f [Accessed: February 10th, 2022]
27. SPECOPS. (2020) The European Countries Most at Risk of Cyber- Crime [Online] Available from: https://specopssoft.com/blog/european-countries-cyber-crime/ [Accessed: March 25,2022].
28. United Nations. (2000) Crimes related to computer networks: Background paper for the workshop on crimes related to the computer network [Online] Available from: https://digitallibrary.un.org/record/432653?ln=en#record-files-collapse-header [Accessed: 5th of February2022]
29. United Nations. (2005). Crimes related to computer networks: Background paper for the workshop on crimes related to the computer [Online] Available from: networkhttps://digitallibrary.un.org/record/432653?ln=en#record-files-collapse-header [Accessed: 5th of February2022].
30. van der Wagen, W., Pieters, W. (2020) The hybrid victim: re-conceptualizing high-tech cyber victimization through actor-network theory. Eur J Criminol 17(4), p. 480–497 Available from: https://doi.org/10.1177/1477370818 812016 [Accessed: 1st of March, 2022]
31. Wall, D. (2001) Crime and the Internet: Cybercrime and cyberfears, 1st edition, Routledge, London