New Species of Criminal Phenomena: Organized Cybercrime

Laura Stanila*

Abstract

ICT (Information and Communication Technology) has spread to all dimensions of social life, including criminal phenomenon. Organized crime, as a rising type of crime, has gained new forms of manifestation since the members of criminal groups use ICT tools to commit crimes or moved to virtual space as this space offers them the ideal "work-field" providing anonymity, a large number of victims, and huge sources of profit.

In fact, the organized cybercriminal groups have become one of the most ascending criminal groups, very difficult to discover and combat.

In the present study, the author offers a presentation of cybercrime in its organized form, presents the cybercriminal groups, their types and characteristics and the types of cybercrimes that are to be committed by an organized criminal group online and offline.

Keywords: *cybercrime, organized crime, organized criminal group, organized cybercrime, cybercriminal group*

I. The Newest Challenge for the Criminal Investigators. Social context

In the recent years everyone may notice an increasing addiction of the society to technology, especially to ICT (Information and Communication Technology). This addiction turned dramatic as it has extended in the "criminal" area with criminals becoming specialized in committing online crimes and in using AI (artificial intelligence) as an important tool to achieve illegal goals. Organized crime was itself a devastating plague of the contemporary society, very difficult to discover, investigate and combat, but the new social realities seem to make it even more dangerous and even more difficult to fight with. Digital networks seem the perfect playground for criminals taking advantage of their features and advantages: privacy, secrecy, velocity, the possibility for dissimulation. Due to these features, the criminal goal is easier to achieve, while *modus operandi* is changed and adapted to the digitalization of the society. The result of this tendency is a sad one: a new type of organized crime – organized cybercrime.

As general Director of the FBI had stated *"transnational crime groups, sexual predators, fraudsters, and terrorists are all transforming the way they do business as technology evolves. Huge swaths of these crimes have a digital component or occur almost entirely online. And new technical trends are making the investigative environment a lot more complex"*[1].

* PhD, Associate Professor, West University of Timişoara (Romania). Contact: laura.stanila@e-uvt.ro.

[1] C. Wray, Director of Federal Bureau of Investigation (FBI), *Digital Transformation: Using Innovation to Combat the Cyber Threat*, Speech at the Boston College/FBI – Boston Conference on Cyber Security, March 7, 2018, https://www.fbi.gov/news/speeches/digital-transformation-using-innovation-to-combat-the-cyber-threat, accessed on 2.11.2020.

II. What is cybercrime? What is organized cybercrime? Distinctions

Cybercrime has evolved in parallel with society's use of digital networks, reacting to every development in legal sector with new approaches to committing offenses[2]. Scholars have noticed that, in the past decade, cybercrime has transformed itself from fragmented acts committed by individuals to increasingly sophisticated and highly professionalized activity[3].

It is obvious we are facing a new type of organized criminal groups operating solely in the cyberspace, tending to expand their activity at a global level.

From the very beginning one should notice that nowadays several terms and expressions are used in relation with the notion of crime in cyberspace and the notion of organization of crime. For example, would it be accurate to refer to organized cybercrime as organized crime in cyberspace? Or do these notions differ?

The answer key to this question is the cyberspace.

a) If we consider cyberspace as a medium for "traditional organized crime", a space where organized crime carries out its activity, then organized cybercrime is in fact a subdivision, a special type of organized crime.

In this case, the structure, purpose and operations of organized crime are the same in the case of organized cybercrime, while the area of carrying out criminal operations, the IT specializations of the members of the organized criminal group and a specific modus operandi implying specific techniques and methods (e.g. phishing, botnet trade) are features characterizing organized crime in cyberspace.

b) If we consider cyberspace as an enabler for organized crime, then organized cybercrime becomes a new distinct type of crime, which shares few features with traditional organized crime.

The debate on this distinction is not new. Actually, in the early 2000s, there were scholars affirming organized crime and cybercrime could not be one and the same because organized crime would be operated offline while most cybercrimes would be committed by individuals rather than organized groups[4]. Williams even identified five possible trends in the evolution of organized crime in the era of digitalization:

1. the use of the Internet for major fraud and theft activities by the organized crime groups;

2. the increased opportunities for profit stemming from the growth of electronic banking and electronic commerce for organized crime.

3.the growth of cyberextortion using complex extortion schemes, conducted anonymously and incurring modest risks, very efficient in money outputs.

4. the use of "nuisance tools", such as computer viruses, for more openly criminal activities.

5. jurisdictional arbitrage – cybercrimes will be committed by organized criminal groups in jurisdictions with poor legal framework and little capacity to enforce laws against cybercrime.

---

[2] T. Tropina, *The evolving structure of online criminality. How cybercrime is getting organized*, Eucrim, The European Criminal Law Associations' Forum, issue 4/2012, p. 158.

[3] *Idem*.

[4] P. Williams, *Organized Crime and Cybercrime: Synergies, Trends, and Responses*, Global Issues, Volume: 6, Issue: 2, August 2001, pp. 22-26, https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=191389, accessed on 2.11.2020.

6. the increased use of the Internet for money laundering, as being a medium through which international trade takes place. Online auctions and online gambling offer similar opportunities to launder money through apparently legitimate purchases, and then lose the "clean" money through offshore financial centers. In addition, *"as e-money and electronic banking become more widespread, the opportunities to conceal the movement of the proceeds of crime in an increasing pool of illegal transactions are also likely to grow"*[5].

7. growing network connections between hackers or small-time criminals and organized crime. Network connections between the two kinds of groups are likely to deepen and widen.

Referring to all trends, it is worth to mention organized crime groups use the Internet for communications (usually encrypted) and for other purposes. Organized crime is proving as flexible and adaptable in its exploitation of cyber-opportunities as it is in any other opportunities for illegal activity.

These thoughts were expressed 18 years before and they appear accurate in the contemporary context.

In 2017 a study was conducted to investigate to what extent cybercriminals operating in phishing and malware attacks can be conceptualized as organized criminal groups. To answer this question, the authors analyzed 40 criminal networks investigated in four countries (Netherlands, UK, USA and Germany) and analyzed them through an organized crime analytical framework. The empirical analysis indicates that even if the criminal networks considered display the minimum set of characteristics to consider them as organized crime, if someone looks only at their structure and composition, they mostly fail to meet the existing definitions of organized crime when it comes to the characteristics of criminal activities carried out and social functions of these networks[6].

As a result of the study, the authors identified 39 networks and classified them into four types:

1. Completely through offline social contacts;
2. Offline social contacts as a base and online forums to recruit specialists;
3. Online forums as a base and offline social contacts to recruit local criminals;
4. Completely through online forums.

The analysis revealed specific features of traditional organized crime, such as use of Violence and Corruption and connections with the Legal Economy. Still, it was very difficult to declare cybercriminals operating in phishing and malware attacks, which were indeed acting in networks, as organized criminal groups.

Tropina distinguishes between two different phenomena, namely, migration of traditional organized crime in cyberspace and organized groups focused on committing cybercrimes[7]:

a) migration of traditional organized crime in cyberspace

The Internet has become a tool for facilitating all types of offline organized criminality (child abuse, drug trafficking, trafficking in human beings for sexual exploitation, illegal migration, different types of fraud, and counterfeiting) due to increased anonymity, money laundering schemes and possibilities of advertising.

---

[5] *Idem*.

[6] E.R. Leukfeldt, A. Lavorgna, E.R. Kleemans, *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime, European Journal of Criminal Policy Res* 23, 2017, pp. 287–300, https://doi.org/10.1007/s10610-016-9332-z, accessed on 2.11.2020.

[7] T. Tropina, *cited,* p. 159.

b)organized groups focused on committing cybercrimes.

This is a new form of organized crime characterized as organized structures operating solely in global information networks and committing only cybercrimes. This new type of organized crime is also characterized by different, constantly evolving structures and new ways of using hi-tech tools in order to obtain illegal profits.

These two types of organized crime coexist, with an increasing ascension of the latter.

The global security strategist and expert Marc Goodman, in an interview in 2015 said that the old image of a hacker was that of a "*17-year-old kids living in their parents' basements. Today, the average age of a cybercriminal is 35, and 80% of black-hat (e.g., criminal) hackers are affiliated with organized crime. (...) In other words, people are choosing this as a profession. (...)That's a radical shift, and it's led to the creation of increasingly sophisticated criminal organizations that operate with the professionalism, discipline, and structure of legitimate enterprises"*[8].

In order to illustrate the importance of the topic, we exemplify with a criminal organization known as Innovative Marketing that created a malware program it disguised as antivirus software. Using its crimeware tool to hijack Internet users' Web browsers, Innovative Marketing deceived hundreds of thousands of people into disclosing their credit card numbers and buying its fake antivirus software. This criminal enterprise operated for three years before being shut down by the FBI and Interpol, both of which calculated its fraudulent sales of malicious software at over 100 million dollars. Innovative Marketing maintained a headquarters in a three-story office building in the Ukraine and even had an org chart with a CEO, CFO, CIO, and head of HR. HR was responsible for hiring mules and bringing criminals into the organization. The CIO was responsible for the dark Web infrastructure that enabled the company to operate clandestinely on the Internet. Innovative Marketing also had a quality assurance team that tested its malicious code against over 200 legitimate antivirus programs before releasing it. At its height, the "company" had more than 600 employees and operated in more than 60 countries[9].

III. Types of organized cybercrime groups

In 2012, it was stated that about 80% of cybercrime could be the result of some form of organized activity[10].

The scholars have identified six basic organizational patterns of cybercrime, however noted that the typology of organized cybercrime groups is likely to change as the digital environment evolves[11].

---

[8] The Wall Street Journal, *Security Expert Marc Goodman on Cyber Crime*, May 12, 2015, https://deloitte.wsj.com/cio/2015/05/12/security-expert-marc-goodman-on-cyber-crime/, accessed on 2.11.2020.

[9] US Attorney's Office, *Northern District of Illinois, U.S. Indicts Ohio Man and Two Foreign Residents in Alleged Ukraine-Based "Scareware" Fraud Scheme That Caused $100 Million in Losses to Internet Victims Worldwide*, May 27, 2010, https://archives.fbi.gov/archives/chicago/press-releases/2010/cg052710-1.htm, accessed on 2.11.2020.

[10] M. McGuire, *Organised Crime in the Digital Age*, London, John Grieve Centre for Policing and Security, 2012.

[11] Idem. Also see M. Mazela, *Organizational structures of cybercrime groups: Overview of key characteristics*, European Cybersecurity Market, Volume 2, Issue 3-4, 2018, pp.18-23.

a) Type I groups operate solely online, being mostly "virtual" while trust is assessed via reputation in online illicit activities. This category includes two subtypes: swarms and hubs[12].

a.1. Swarms appear as "disorganized organizations with common purpose and without leadership". They are types of networks and have minimal chains of command, acting essentially online. Sworms *"may operate in viral forms in ways reminiscent of earlier 'hacktivist' groups"*[13]. They are most active in ideologically driven online activities (e.g. hate crimes, political resistance). The group Anonymous illustrates a typical swarm-type group[14].

a.2. Hubs are essentially active online also, however they have a command structure, being more organized than swarms. They involve a focal point (hub) of core criminals around which peripheral associates gather. Their activities are very diverse – phishing attacks, botnets, online sexual offending etc., all of them happening online. An example of hub-type cybercriminal group is Silk Road 2.0[15], which is an online market trading in illicit goods such as drugs.

b) Type II groups operate both online and offline and are described as "hybrids". This category could be also divided into two subtypes: clustered hybrids and extended hybrids.

b.1. the *clustered hybrid* is characterized by criminal acts committed by a small group of individuals using specific activities or methods. Clustered hybrids resemble with hubs in their structure, but oscillate between online and offline criminal acts. Their activities are driven by profit. An example of a sophisticated cybercriminal hub/ clustered hybrid and its organization was presented by Chabinsky, a representative of the US Federal Bureau of Investigation's Cyber Division, during his speech[16]: *"Coders create malware, exploits, and other tools necessary to commit the crime. Distributors trade/sell stolen data and vouch for the goods provided by the other specialties.*

---

[12] R. Broadhurst, P. Grabosky, M. Alazab, S. Chon, *Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime*, International Journal of Cyber Criminology, Vol 8, Issue 1, January – June 2014, p. 7.

[13] P.Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency,* London: Little, Brown, 2012.

[14] *Anonymous* is a network of thousands of activists, a minority of them hackers, devoted to leftist-libertarian ideals of personal freedom and opposed to the consolidation of corporate and government power. *See* Dale Beran, The Return of Anonymous. The infamous hacker group reemerges from the shadows, The Atlantic, August 11, 2020, https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymous-returns/615058/, accessed on 3.11.2020.

[15] *Silk Road 2.0* is an underground website, lauched in 2013 and owned by Blake Benthall, aka "Defcon", being one of the most extensive, sophisticated, and widely used criminal marketplaces on the Internet today. The website has operated on the "Tor" network, a special network of computers on the Internet, distributed around the world, designed to conceal the true IP addresses of the computers on the network and thereby the identities of the network's users. Since its launch in November 2013, Silk Road 2.0 has been used by thousands of drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other illicit goods and services to buyers throughout the world, as well as to launder millions of dollars generated by these unlawful transactions. As of September 2014, Silk Road 2.0 was generating sales of at least approximately $8 million per month and had approximately 150,000 active users. *See* J. Cook, *FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0*, Business Insider, November 6, 2014, https://www.businessinsider.com/fbi-silk-road-seized-arrests-2014-11, accessed on 3.11.2020.

[16] S. Chabinsky, *The Cyber Threat: Who's Doing What to Whom?* Federal Bureau of Investigation, 2010, Retrieved from https://archives.fbi.gov/ archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom, accessed 5.11.2020.

Technicians maintain the criminal infrastructure and supporting technologies. Hackers search for and exploit vulnerabilities in applications, systems, and net- works in order to gain administrator or payroll access. Fraud specialists develop and employ social engineering schemes, including phishing, spamming, and domain squatting. Hosts provide "safe" facilities of illicit content servers and sites. Cashers control drop accounts and provide those names and accounts to other criminals for a fee; they also typically manage individual cash couriers, or "money mules." Money mules transfer the proceeds of frauds which they have committed to a third party for further transfer to a secure location. Tellers assist in transferring and laundering illicit proceeds through digital currency ser- vices and between different national currencies. Executives of the organization select the targets, and recruit and assign members to the above tasks, in addition to managing the distribution of criminal proceeds."

b.2. *extended hybrids* act similarly to clustered hybrids but are less centralized. They typically include many associates and subgroups and carry out a variety of criminal activities, but still retain a level of coordination sufficient to ensure the success of their operations. The level of coordination is based on the complexity of the operation. Their activities are also driven by profit.

c) Type III groups operate offline but use online technology and cyberspace to run their offline activities. They are increasingly contributing to digital crime and can be subdivided into "hierarchies" and "aggregates", due to their degree of organization and cohesion.

c.1. *Hierarchies* are traditional organized criminal groups which export some of their activities online, using the Internet to support/expand their offline activities. Examples include online gambling, blackmail, extortion, prostitution moved online (pornography, webcams) etc.

c.2. *Aggregates* are superficially organized, temporary, and often without clear purpose groups. They use digital technologies ad hoc. E.g. the use of Blackberry Messenger to coordinate public disorder during the 2011 UK riots[17]. The Sydney riots in September 2012[18] were conducted in the same way.

Also, organized cybercrime group could be classified regarding the purpose criteria in other two subtypes[19]:

a) enterprise or profit-oriented activities, and especially cybercrime committed by state actors, appear to require leadership, structure, and specialization.

b) protest activity tends to be less organized, with weak (if any) chain of command.

IV. Features of the organized cybercrime groups

The doctrine has noted that half of the cybercrime groups in his sample comprised six or more people, with one-quarter of groups comprising over 10 individuals. One-quarter of cybercrime groups had operated for less than 6 months. However, the size

[17] J. Halliday, *London riots: BlackBerry to help police probe Messenger looting 'role'*, The Guardian, August 8, 2011, retrieved from https://www.theguardian.com/uk/2011/aug/08/london-riots-blackberry-messenger-looting, accessed 5.11.2020.

[18] ABC News, *As it happened: Violence erupts in Sydney over anti-Islam film*, September 15, 2012, retrieved from https://www.abc.net.au/news/2012-09-15/anti-us-protests-hit-sydney/4263372, accessed 5.11.2020.

[19] R. Broadhurst et all., cited, p. 1.

of the group or the duration of their activities did not predict the scale of offending, as small groups can cause significant damage in a short time[20]. The scholars also noted a substantial functional specialization and divisions of labor as specific features of the organized cybergroups.

In fact, the main features identified by the doctrine for the organized cybercrime groups and the activity of their members are[21]:

- Coders or programmers write the malware, exploits, and other tools necessary to commit the crime.
- Distributors or vendors trade and sell stolen data, while vouch for the goods provided by the other specialties.
- Technicians maintain the criminal infrastructure and supporting technologies, such as servers, ISPs, and encryption.
- Hackers search for and exploit vulnerabilities in applications, systems, and networks in order to gain administrator or payroll access.
- Fraud specialists develop and employ social engineering schemes, including phishing, spamming, and domain squatting.
- Hosts provide "safe" facilities of illicit content servers and sites, often through elaborate botnet and proxy networks.
- Cashers control drop accounts and provide those names and accounts to other criminals for a fee; they also typically manage individual cash couriers, or "money mules."
- Money mules transfer the proceeds of frauds which they have committed to a third party for further transfer to a secure location.
- Tellers assist in transferring and laundering illicit proceeds through digital currency services and between different national currencies.
- Executives of the organization select the targets, and recruit and assign members to the above tasks, in addition to managing the distribution of criminal proceeds.

This ideal type is not necessarily limited to a formal, fixed organization. Some functions may be outsourced. The organization of cybercrime may also occur at a wider level involving networks of individuals who meet and interact within online discussion forums and chat rooms, some of them functioning as virtual black markets that advertise illicit goods or services.

According to Wall[22] cybercriminal groups share at least one of the following features:

- structure
- members have specific skill sets
- members exercise different responsibilities within the group;
- members are involved in the activity of two or more groups simultaneously;
- members worked with the same group on a regular basis, but on different occasions;
- members act together to commit the same type of crime, or share interests and/or common goals;
- members are self-contained;

---

[20] M. McGuire, cited.

[21] S. R. Chabinsky, *The Cyber Threat: Who's Doing What to Whom?* FBI, 2010, March 23, retrieved on 15th December 2013 from http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom.

[22] D. Wall, *Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime*, The European Review of Organised Crime, 2(2), 2015, pp. 71-90.

- members usually driven by an individual or a very small group;
- adaptability – members are very reactive in response to circumstances;
- members are bound together by reputational economy.

According to Leukfeldt, Lavorgna and Kleemans[23] the cybercrime groups share the following features:

- there is no strict hierarchical structure per se.
- dependency relationships between their members
- different functional roles of their members
- three different structural layers: core members (stable group which commit crimes with the same team for a period of time, however, sometimes they simultaneously work with criminals from other groupings), enablers and money mules. In the absence of core members, cybercrime groups use online forums to identify and select suitable co-offenders. In these cases, the members of cybercrime groups have technical expertise, are active on online criminal forums and work together occasionally.
- the groups' structure is based on offline social contacts;
- offline social contacts are used to create the team of core members while online forums were used to recruit specialists.

The doctrine tried to classify the cybercrime groups in the following categories[24]:

- large size groups (more than 21 members)
- medium size groups (5–10 members) which are the most common.
- groups with 11–20 members
- small size groups (2–4 members)

A more complex classification of Cybercrime groups is presented in the Comprehensive Study on Cybercrime of UNDOC – United Nations Office on Drugs and Crime in 2013[25]: groups with 2 members, groups with 3-5 members, groups with 6-10 members, groups with 11-20 members, groups with over 20 members.

It is worth to mention that typology of cybercrime groups is continuously evolving, making it very difficult to identify and combat. The judicial bodies must monitor and analyze each group, focusing on the following elements[26]:

- size of the group;
- strength of association between the members;
- environment where the group operates;
- tools the group uses;
- group's financial resources;
- profile of the victim;
- members' responsibilities;
- hierarchy within the group;
- group's goal;
- using 'crime as a service';

---

[23] E.Leukfeldt, A.Lavorgna, E. Kleemans, *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, *European Journal on Criminal Policy and Research*, 23(3), 2016, pp.287-300.

[24] M. Mazela, cited, p. 22.

[25] Malby et. all, cited, p. 48; *Comprehensive Study on Cybercrime of UNDOC – United Nations Office on Drugs and Crime* p. 3.

[26] Malby, cited, p. 23.

- reactiveness in response to circumstances;
- importance of reputational economy;
- working with multiple groups at the same time;
- time frame of the cooperation;
- social relationships between the members.

V. Priorities of Europol: Organized Cybercrime

In its 2019 Internet Organized Crime Threat Assessment Report – IOCTA[27], Europol's European Cybercrime Centre (EC3) provides key recommendations to law enforcement, policy makers and regulators to allow them to respond to cybercrime in an effective and concerted manner. The IOCTA Report focuses on cybercrime priorities, which are determined by the EU Policy Cycle – EMPACT, are currently: Cyber-dependent crime, online child sexual exploitation and payment fraud. Further, the preoccupation of the EUROPOL also focuses on the criminal abuse of the dark web, the convergence of cyber and terrorism and on cross-cutting crime factors.

a) Cyber-dependent crime

While ransomware remains the top threat in this report, the overall volume of ransomware attacks has declined as attackers focus on fewer but more profitable targets and greater economic damage. Also, the report speaks about *phishing* and *vulnerable remote desktop protocols (RDPs)* being the key primary malware infection vectors. In addition data remains a key target, commodity and enabler for cybercrime. Following the increase of destructive ransomware, such as the German wiper attacks of 2019, the report states there is a growing concern within organizations over attacks of sabotage making continuous efforts needed to further synergize the network and information security sector and the cyber law enforcement authorities improving the overall cyber resilience and cybersecurity.

b) online child sexual exploitation

The 2019 IOCTA Report states the amount of child sexual exploitation detected online by law enforcement and the private sector had continued to increase, putting considerable strain on law enforcement resources. There is an increased online solicitation of children for sexual purposes with a largely unchanged modus operandi, facilitated by growing access of minors to high quality smartphones and a lack of awareness of the risks.

c) payment fraud

Skimming continues to evolve with criminals continuously adapting to new security measures while jackpotting attacks are becoming more accessible and successful.

d) criminal abuse of the dark web

The dark web remains the key online enabler for trade in an extensive range of criminal products and services and a priority threat for law enforcement. The coordinated law enforcement activities, combined with extensive Distributed Denial of Service (DDoS) attacks have generated distrust in The onion router (Tor) environment. There is strong evidence administrators are exploring alternatives, but a full

[27] EUROPOL, *Internet Organized Crime Threat Assessment 2019* (IOCTA 2019), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019, accessed on 5.11.2020.

migration to new platforms is unlikely just yet, due to the user-friendliness, existing market variety and customer-base on Tor. Some organized crime groups are also fragmenting their business over a range of online marketplaces, while encrypted communication applications enhance single-vendor trade on the dark web, helping direct users to illegal services and enabling closed communications.

e) the convergence of cyber and terrorism

Terrorist groups adopt new technologies, exploit emerging platforms for their online communication and distribution strategies and other online service providers also. Online medium offers perfect conditions for planning and recruiting new members, terrorist attacks can rapidly turn viral, making law enforcement difficult to quickly respond.

f) cross-cutting crime factors

Phishing remains an important tool in the arsenal of cybercriminals for both cyber-dependent crime and non-cash payment fraud, while cryptocurrencies continue to facilitate cybercrime.

Previously, in 2010, the EU set up a four-year policy cycle in order to create a greater measure of continuity for the fight against serious international and organized crime. EU Policy Cycle – EMPACT priorities for the fight against organized and serious international crime between 2018 and 2021 were adopted by the Council of the EU at its meeting on 18 May 2017, and among them stands the fight against cybercrime. In order to achieve this goal, several directions were established[28]:

a. disrupting the criminal activities related to attacks against information systems, particularly those following a Crime-as-a-Service business model and working as enablers for online crime;
b. combating child sexual abuse and child sexual exploitation, including the production and dissemination of child abuse material, *and*
c. targeting criminals involved in fraud and counterfeiting of non-cash means of payment, including large-scale payment card fraud (especially card-not-present fraud), emerging threats to other non-cash means of payment and enabling criminal activities.

Europol's European Cybercrime Centre (EC3) defines cyber-dependent crime as *"any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT)".*

The 2019 Europol Report reveals the top European cybercrime treats, trends and areas for law enforcement improvement.

Finally, Internet Organized Crime Threat Assessment Report – IOCTA 2020[29] has emphasized a new cross-cutting crime facilitator – COVID 19 pandemic: *"the outbreak of COVID-19 has demonstrated the unfortunate impact potential of such crises on our daily lives across the globe. As physical lockdowns became the norm, cybercrime became more popular than before. There is no denying that the arrival of COVID-19 was a crucial factor in any development discussed with respect to 2020. However, COVID-19 in connection to cybercrime needs to be placed within its context. If anything, COVID-19 demonstrated how cybercrime – at its core – remains largely the same but criminals*

[28] Europol – EU Policy Cycle – EMPACT, https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact, accessed on 6.06.2020.

[29] Europol, *Internet Organized Crime Threat Assessment 2020* (IOCTA), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020, accessed on 5.11.2020.

change the narrative. They adapt the specifics of their approach to fit the societal context as a means to enhance their rate of success."[30] At the same time, the pandemic *"also gave rise to disinformation campaigns and activities. Disinformation efforts are often associated with hybrid threats, which are defined as threats combining conventional and unconventional, military and non-military activities which may be used by non-state or state actors to achieve political aims. A wide range of measures applied in hybrid campaigns include cyber-attacks and disinformation, disruption of critical services, undermining of public trust in governmental institutions and exploiting social vulnerabilities. The presence of disinformation became a crucial feature in the overall threat landscape during the crisis"*[31].

V. Types of tools and methods used by organized cybercrime groups

Organized cybercrime uses specific tools and methods applied by specialized members who act mainly online. The most common of these tools and methods were reported the following[32]:

a) Ransomware

Ransomware maintained as the top cyber threat in Europe in the 2019 and 2018. The primary methods used by malicious cyber actors to compromise networks include social engineering and highly targeted phishing emails (*spear-phishing*), the use of vulnerable remote desktop protocols (RDPs) – either through hacking or buying access to the network through a criminal forum and destructive cyber acts of sabotage, designed to cause permanent destruction of the victim's data, such as the *GermanWiper*[33] malware which surfaced in 2019.

b) Data compromise

Data compromise refers to illegally obtained financial or personal data through means such as malware or phishing. After ransomware, the compromise of data represents the second most prominent cyber threat in Europe. This data may be used directly to commit fraud or sold to other criminals on the dark web. Whilst compromised financial data may allow for immediate financial gains by cyber criminals, personal data may be used to enable targeted attacks such as spear-phishing or Business Email Compromise (BEC) fraud, which in the longer term may yield more significant criminal proceeds.

There is also a growing threat of malicious insider activity in compromising data, where the insider works directly for a company or for a third-party service provider.

---

[30] IOCTA 2020 p. 13.

[31] IOCTA 2020 p. 13.

[32] N.G. Miralis, *What were the greatest organised cybercrime threats in 2019?*, Lexology, February 14, 2020, https://www.lexology.com/library/detail.aspx?g=8ca91844-7c49-4542-9a7a-f78530b616dc, accessed on 5.11.2020.

[33] *GermanWiper* was a ransomware which didn't encrypt files but instead it rewrote their content with zeroes, permanently destroying users' data. As a result, any users who got infected by this ransomware should have been aware that paying the ransom demand would not helped them recover their files. Unless users had had created offline backups of their data, their files were gone and unrecoverable. *See* C. Cimpanu, *GermanWiper ransomware hits Germany hard, destroys files, asks for ransom*, ZD Net, 2 August 2019, retrieved from

https://www.zdnet.com/article/germanwiper-ransomware-hits-germany-hard-destroys-files-asks- for-ransom/, acessed on 10.03.2020.

c) DDoS attacks

Distributed Denial of Service (DDoS) attacks occur where multiple compromised systems work together to deny others access to an entity's data or services, critically disrupting the operations of an organization. DDoS attacks were identified as the third most significant threat in the Report. Whilst attacks were most commonly motivated by financial gain through extortion, other attacks were of an ideological/political nature or purely malicious.

d) Attacks on critical infrastructure

These attacks may involve the use of some of the previously covered attack tools such as DDoS, however they are distinguished by the primary motive focusing on attacking the infrastructure itself and disrupting its functions.

e) Website defacement

The number of website defacement cases still requires the allocation of limited law enforcement resources. Investigation of these offences may help to catch potential future cybercriminals testing out their capabilities and prevent them from developing a career in cyber crime.

f) Lower priority threats

This category includes data stealing malware, cryptomining by exploiting a victim's processing power without their permission to mine cryptocurrencies and mobile malware.

g) Future threats and developments

In the future there will likely be a growth in supply chain attacks, financially motivated cybercrime focused on cryptocurrency assets and significant ongoing risk to the Domain Name System (DNS) infrastructure allowing malicious actors to see data in transit, redirecting traffic or spoofing[34] specific websites.

VI. Types of cybercrime committed by organized groups

Cybercrime was defined as computer-related crime, its development being closely related and influenced by the global connectivity. Cybercrime activities are characterized by the use of globalized information communication technology (ICT) for committing criminal acts. Another important feature is its transnational spread and its transnational outcome.

Still, some scholars[35] do not use the term "computer crime" because its narrowness, using instead only the term "cybercrime", the prefix "cyber" emphasizing that both computers *and* the Internet are inextricably linked with the crime. Thus Cybercrime is defined as *"criminal acts committed using electronic communication networks and information systems or against such networks and systems"*[36]. Based on this definition, cybercrimes can be distinguished as:

1. target cybercrimes: crimes in which a computer is the target of the offense; and
2. tool cybercrimes: crimes in which a computer is used to facilitate a traditional crime.

---

[34] *Spoofing* a website means creating a website as a hoax, with the intention of misleading readers that the website has been created by a different person or organization.

[35] J.-J.Oerlemans, *Investigating Cybercrime*, Thesis, SIKS – The Dutch Research School for Information and Knowledge Systems, Amsterdam University Press, 2017, p. 20, DOI: 10.13140/RG.2.2.19060.55686.

[36] *Ibidem*.

The scholars have tried to identify the types of cybercrime committed by organized groups, even if there is lack of a general definition of cybercrime itself[37].

a) Acts against the confidentiality, integrity and availability of computer data or systems, including:
   - Illegal access to a computer system;
   - Illegal access, interception or acquisition of computer data;
   - Illegal interference with a computer system or computer data;
   - Production, distribution or possession of computer misuse tools
   - Breach of privacy or data protection measures;

b) Computer-related acts for personal or financial gain or harm, including:
   - Computer-related fraud or forgery;
   - Computer-related identity offences;
   - Computer-related copyright or trademark offences;
   - Sending or controlling sending of Spam;
   - Computer-related acts causing personal harm;
   - Computer-related solicitation or 'grooming' of children;

c) Computer content-related acts, including
   - Computer-related acts involving hate speech;
   - Computer-related production, distribution or possession of child pornography;
   - Computer-related acts in support of terrorism offences;

However, this list is not exhaustive and could be detailed, including in the first category the following[38]: *illegal access to a computer system; illegal access, interception or acquisition of computer data;illegal data interference or system interference; production, distribution, or possession of computer misuse tools; breach of privacy or data protection measures*; *computer-related fraud or forgery;computer-related identity offences; computer-related copyright and trademark offences; sending or controlling sending of spam; computer-related acts causing personal harm; computer-related acts involving racism or xenophobia; computer-related production, distribution, or possession of child pornography; computer-related solicitation or 'grooming' of children; computer-related acts in support of terrorism offences.*

VII. Predictions on cybercrime

The so called "crime's movement into cyberspace" affected the structure of organized criminal activity. Cyberspace frees individuals from many of the constraints that apply to activities in the real world, thus many forms of criminal organizations have made the transition to online crime. In the cyberworld, acts and processes are mostly automated, real-world physical force being unlikely to play a significant role in online criminal activities. As Brenner stated, "situational concentrations of effort are far more easily achieved in cyberspace than in the real world. Activity in cyberspace is not constrained by geography or other temporal limitations. Indeed, even time is less of a constraint in cyberspace, where processes can be automated and monitored only sporadically". At the same time, hierarchical structure of a traditional organized criminal group evolved to allow criminal groups to carry out large-scale, complicated

[37] Malby et. all, cited, p. 16.
[38] Malby et. all, cited, *Annex 1 – Act descriptions*, p. 257-258.

entrepreneurial activities both in the real world and cyberspace. However, in cyberspace, the rigid hierarchical structures of traditional organized criminal groups do not fit, since online criminal activity emphasizes lateral relationships and networks instead of hierarchies. Swarms, hubs or hybrid organizational models of cybercrime groups prove to be more adaptable, yet very difficult to identify and combat by judicial bodies. The cybercrime groups may constitute and act ad hoc, only for a short period of time and to complete a specific criminal activity, making them very difficult to include in the traditional organized criminal group, since their features do not fit the features of the latter.

As the doctrine pointed out, "in the real-world, the stability and consistency of organized criminal groups gives law enforcement a fixed target upon which to focus its efforts. Police concentrate on identifying a permanent group of participants who engage in a set of routine illicit activities. This predictability, in itself, enhances law enforcement's ability to combat organized crime making police to lose this advantage, which will only contribute to the success of organized cybercrime"[39].

The efforts and struggle of the judicial bodies in their fight with this new type of organized crime is once more emphasized by the Director of FBI in 2018: "As cyber threats evolve, we need to evolve as well. This means evolving both our day-to-day operational strategies and our broader approach to handling global digital challenges. To combat these blended threats and worldwide computer intrusions, we can no longer just investigate individual parts of a criminal scheme occurring in one jurisdiction. We need to focus our efforts on dismantling the entire cyber enterprise. We're prosecuting the actors, burning their infrastructure, and seizing their illicit proceeds. We're taking down the groups running malware campaigns and the criminals who support them—those who operate the dark markets, compromise networks and servers, and the people who buy and sell stolen data. Think of it as going after the distribution ring and the manufacturer rather than simply taking out the drug dealer on the corner. And we need to have a global perspective. We need to delegate roles and responsibilities across multiple field offices and to international partners—so that we can share information in real time, as we target and dismantle the most significant cyber enterprises"[40].

References

1. ABC News, *As it happened: Violence erupts in Sydney over anti-Islam film*, September 15, 2012, retrieved from https://www.abc.net.au/news/2012-09-15/anti-us-protests-hit-sydney/4263372, accessed 5.11.2020.

2. Beran, D., *The Return of Anonymous. The infamous hacker group reemerges from the shadows*, The Atlantic, August 11, 2020, https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymous-returns/615058/, accessed on 3.11.2020.

3. Brenner, S., *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships*, North Carolina Journal of Law & Technology, Volume 4(1): 1-51, Fall 2002, https://www.researchgate.net/publication/228198960_Organized_

[39] S.Brenner, *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships*, North Carolina Journal of Law & Technology, Volume 4(1):1-51, Fall 2002, pp.47-51, https://www.researchgate.net/publication/228198960_Organized_Cybercrime_How_Cyberspace_May_Affect_the_Structure_of_Criminal_Relationships, accessed on 5.11.2020.

[40] C. Wray, cited.

Cybercrime_How_Cyberspace_May_Affect_the_Structure_of_Criminal_Relationship, accessed on 5.11.2020.

4. Broadhurst, R., Grabosky, P., Alazab, M., Chon, S., *Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime*, International Journal of Cyber Criminology, Vol. 8, Issue 1: 1-20, ianuarie-iunie 2014.

5. Chabinsky, S., *The Cyber Threat: Who's Doing What to Whom?* Federal Bureau of Investigation, 2010, Retrieved from https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom, accessed 5.11.2020.

6. C. Cimpanu, *GermanWiper ransomware hits Germany hard, destroys files, asks for ransom*, ZD Net, 2 August 2019, retrieved from https://www.zdnet.com/article/germanwiper-ransomware-hits-germany-hard-destroys-files-asks-for-ransom/, acessed on 10.03.2020.

7. Cook, J., *FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0*, Business Insider, November 6, 2014, https://www.businessinsider.com/fbi-silk-road-seized-arrests-2014-11, accessed on 3.11.2020.

8. EU Organized Crime Threat Assessment 2007; www.europol.europa.eu.

9. Europol – EU Policy Cycle – EMPACT, https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact, accessed on 6.06.2020.

10. EUROPOL, *Internet Organized Crime Threat Assessment 2019* (IOCTA 2019), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019, accessed on 5.11.2020.

11. Falcone, G., *Mafia*, Ed.Danubius, Bucureşti, 1994.

12. Halliday, J., *London riots: BlackBerry to help police probe Messenger looting 'role'*, The Guardian, August 8, 2011, retrieved from https://www.theguardian.com/uk/2011/aug/08/london-riots-blackberry-messenger-looting, accessed 5.11.2020.

13. https://deloitte.wsj.com/cio/2015/05/12/security-expert-marc-goodman-on-cyber-crime/, accessed on 2.11.2020.

14. Kerr, P., *Mafia Rusească,* Ed. Aldo Press, 1997.

15. Leukfeldt, E.R., Lavorgna, A., Kleemans, E.R., *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime, European Journal of Criminal Policy Res* 23, 2017, https://doi.org/10.1007/s10610-016-9332-z, accessed on 2.11.2020.

16. Longo, F., *Discoursing organized crime. Towards a two-level analysis,* în Felia Allum, Francesca Longo, F., Irrera, D., Kostakos P.A. (editors), *Defining and Defying Organized Crime. Discourse, perceptions and reality,* Part I, Routledge advances in international relations and global politics, Rutledge, New York, 2010.

17. Mazela, M., *Organizational structures of cybercrime groups: Overview of key characteristics*, European Cybersecurity Market, Vol. 2, Issue 3-4: 18-23, 2018.

18. McGuire, M., *Organised Crime in the Digital Age*, London, John Grieve Centre for Policing and Security, 2012.

19. Miralis, N.G., *What were the greatest organised cybercrime threats in 2019?*, Lexology, February 14, 2020, https://www.lexology.com/library/detail.aspx?g= 8ca91844-7c49-4542-9a7a-f78530b616dc, accessed on 5.11.2020.

20. Obokata, T., *Transnational Organized Crime in International Law,* Hart Publishing, Oxford and Portland Oregon, USA, 2010.

21. Oerlemans, J.-J., *Investigating Cybercrime*, Thesis, SIKS – The Dutch Research School for Information and Knowledge Systems, Amsterdam University Press, 2017, p. 20, DOI: 10.13140/RG.2.2.19060.55686.

22. Olson, P., *We Are Anonymous: Inside the Hacker World of LulzSec*, Anonymous, and the Global Cyber Insurgency, 2012, London: Little, Brown.

23. Pitulescu, I., *Crima Organizată*, Ed. Naţional, 1996.

24. Puzo, M., *Sicilianul,* Ed. Politică, Bucureşti, 1997.

25. Sutherland, E.H., *White Collar Crime: The Uncut Version*, Yale University Press, 1983, Business & Economics.

26. The Wall Street Journal, *Security Expert Marc Goodman on Cyber Crime*, May 12, 2015,

27. Tropina, T., *The evolving structure of online criminality. How cybercrime is getting organized*, Eucrim, The European Criminal Law Associations' Forum, issue 4/2012.

28. UN Convention against Transnational Organized Crime, 2000.

29. Ursa, V., *Criminologie*, Ed. Didactico-Ştiinţifică, Bucureşti, 1996.

30. US Attorney's Office, *Northern District of Illinois, U.S. Indicts Ohio Man and Two Foreign Residents in Alleged Ukraine-Based "Scareware" Fraud Scheme That Caused $100 Million in Losses to Internet Victims Worldwide*, May 27, 2010, https://archives.fbi.gov/archives/chicago/press-releases/2010/cg052710-1.htm, accessed on 2.11.2020.

31. Wall, D., *Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime*, The European Review of Organised Crime, 2(2), 2015.

32. Williams, P., *Organized Crime and Cybercrime: Synergies, Trends, and Responses*, Global Issues, Volume: 6, Issue: 2, August 2001, https://www.ncjrs.gov/App/ Publications/abstract.aspx?ID=191389, accessed on 2.11.2020.

33. Wray, C., Director of Federal Bureau of Investigation (FBI), *Digital Transformation: Using Innovation to Combat the Cyber Threat*, Speech at the Boston College/FBI – Boston Conference on Cyber Security, March 7, 2018, https://www.fbi.gov/news/speeches/digital-transformation-using-innovation-to-combat-the-cyber-threat, accessed on 2.11.2020.