European Journal of Social Sciences Studies
ISSN: 2501-8590
ISSN-L: 2501-8590
Available on-line at: www.oapub.org/soc

DOI: 10.46827/ejsss.v6i1.956 Volume 6 | Issue 1 | 2021

THE PHENOMENON OF CYBERCRIME: FROM THE TRANSNATIONAL CONNOTATION TO THE NEED FOR GLOBALIZATION OF JUSTICE

Gianpiero Greco[1,2i], Nicola Montinaro[1]
[1]Ministry of the Interior, Department of Public Security, State Police, Milan, Italy
[2]orcid.org/0000-0002-5023-3721

Abstract:
Information technology has brought about epochal changes in every area of society, offering opportunities for development on a social, cultural, and economic level, but also a fertile ground for activities with criminal purposes that take place in cyberspace. The threat present in the intangible world of cyberspace is extremely concrete and is one of the major sources of concern and investment by States, given that the Internet is considered the critical infrastructure for excellence. Cybercrime, characterized by a transnational connotation of borderless or aspatial crime, provides a position of advantage to the cybercriminal compared to the traditional criminal. The development of information technologies has led to the digitization of organized crime which thus succeeds in maximizing profits by exploiting the opportunities offered by new communication technologies and minimizing the risk of being identified, arrested, convicted and of suffering the seizure of the proceeds of criminal activities. Considering the contradictory and inhomogeneous international legal framework due to the transnational scope of cybercrime, the identification of the *locus commissi delicti* is difficult and the legal prosecution of cybercrimes is complex; therefore, cybercriminals could operate without an adequate response from some states in terms of prevention, sanction, containment and contrast. The sovereignty of States, in the context of cybercrime repression, is identified as an insurmountable obstacle in the creation of a supranational union of law. Therefore, to put legal operators in the real conditions to suppress transnational cybercrime, globalization of justice is needed.

Keywords: cyberspace; criminal law; organized crime; crime globalization; transnational crime

[i] Correspondence: email gianpierogreco.phd@yahoo.com

1. Introduction

The development of information technology has brought about epochal changes in every sector of society in recent years. Technology offers multiple opportunities for development on a social, cultural and economic level, but it represents a fertile ground for new methods of aggression against legal assets, having criminal relevance; therefore, this new frontier in the fight against crime generated by information technology can offer innovative tools and means for finding evidence and, in general, for combating serious criminal phenomena. If on the one hand, we have the development of *Information and Communication Technology*, on the other we have the new pathology of *cybercrime*, understood as the complex of actions with criminal purposes, which are perpetuated in *cyberspace* (e.g., computer fraud, identity theft, ransomware extortion, online money laundering, etc.). Cybercrime can therefore be considered a phenomenon that is the result of the evolution of information technology itself that has brought with its security problems (Floridi, 2012).

The transnationality of the cybercrime phenomenon represents a great challenge for States since the shift from a tangible and material environment to an intangible and dematerialized environment means that the crimes committed and the tools and methods used to investigate them are no longer subject to traditional and pre-established rules. The regulations governing traditional means of communication are today, in the face of the new virtual domain coinciding with the cyberspace, inadequate and obsolete, as they are built by referring to a physical and territorial space. Therefore, it is difficult to extend these regulations to include the actions carried out in the cybernetic environment, as this is delocalised and aterritorial in nature. Until now, every criminal organization, even those capable of branching out on an extraterritorial level, was born from and on a specific territory. These organizations identified themselves precisely with their territory of origin, on which they were rooted with their cultural codes, with their traditions. These organizations were characterized by a close bond and direct knowledge between the members. Cybercrime, on the other hand, is distinguished by the transnational connotation of borderless or a-spatial crime, an unprecedented feature among all crimes, which finds no precedent in the history of traditional criminal activities and which makes it the crime for the excellence of the third millennium (Faga, 2017). Another peculiar feature of the criminal threat in cyberspace is the distance between cybercriminals and their potential victims. Illegal conduct can take the form of several actions, carried out at different times or simultaneously by several agents or one in a variety of places or a virtual space. One or more victims may be hit by the cyber-attack, either immediately or after a period (Pansa, 2004). Finally, the cybercriminal is in a position of advantage over the traditional criminal.

2. The digital revolution and related issues

The development of digital technologies, which allows the production, processing, dissemination, transmission and use of information, has undoubtedly resulted in an acceleration of the daily life and lifestyle of the individual, favouring communications and fast connections and global, which are shaping modern society, making it digital (Balsano & Del Monte, 2013). Information and communication technologies are transversally penetrating all productive sectors and systems that regulate social dynamics: public services, knowledge, media convergence, social networks, environmental management, energy problems, agriculture, and the working world. According to the Global Digital 2018 report of 'We Are Social' (2019), out of 7.6 billion inhabitants on the planet, there are 4 billion users connected to the Internet (53% of the world population), and of these, 3.2 billion (42%) are active on social media. This data can allow us to understand how great the criminal impact on the so-called Internet galaxy can be. In particular, for young people, the exposure to digital far exceeds that of school attendance and, even, that dedicated tonight rest, so the media can be transformed into 'weapons of mass distraction', with evident repercussions on preparation school, social relationships and also on the psyche (Teti, 2018).

The so-called *information age* presents great opportunities for humanity as a whole but has also paved the way for risks, threats of all kinds, events that are difficult to predict and conflicts between individual, collective, state or security interests. Technological progress has made available numerous means that greatly expand the range of human potential, but without the necessary adjustments to the ethical and regulatory framework. In this context, the exponential growth of information technologies, unbalanced by adequate legal regulation, has generated a grey space where it is possible to act with impunity for anti-social purposes, ranging from cybercrime to cyber-war (Faga, 2017; Rapetto & Di Nunzio, 2001).

The national and international regulations governing traditional means of communication (radio, press, television, publishing) are, in the face of the new dimension of the cyberspace, profoundly inadequate, as they have been devised thinking of territorial space and therefore it is complex extend them to include operations carried out through the Net; the latter creates a virtual space consisting of websites and web pages that are not located in a specific physical location. The law-cyberspace relationship produces, therefore, a series of relevant problem profiles including those related to the identification of the criminal action and the location of the perpetrator of the cybercrime. The incessant evolution, but also the new needs of globalization and the birth of new legal assets, hitherto unknown, are factors of rapid ageing of the rules and pose to the jurist the problem of a constant search for new rules that better balance the different interests. The digital revolution should, therefore, correspond to an ethical-regulatory evolution aimed at making the same revolution usable in safety (Teti & Caligiuri, 2015).

3. The cyberspace and fundamental issues

The technological substratum where one of the new manifestations of today's crime is perpetuated, as well as a crucial element for the political, social, financial, and human dynamics of the 21st century, is *cyberspace* (Teti & Caligiuri, 2015). It represents a new "aspatial", "deterritorialized", "decentralized" dimension (Levy, 1995) and characterized by the simultaneity, anonymity, "depersonalization" and "detemporalization" of activities (Martino, 2018). According to the 'National strategic framework for the security of cyberspace' (NSFSCS, 2013), the cyberspace is *"the set of interconnected IT infrastructures, including hardware, software, data and users, as well as logical relationships, however established, between them. It, therefore, includes the Internet, communication networks, the systems on which the computer processes of data processing are based, and mobile devices equipped with network connections. […]. It constitutes a virtual domain of strategic importance for the economic, social and cultural development of nations"* (2013); fascinating domain, which represents one of the most critical fields of international politics today and potentially tomorrow, as well as a concrete threat to national and international security.

Cyberspace penetrates transversally into all productive sectors and systems that regulate social dynamics: public services, knowledge, social networks, environmental management, air, sea and rail traffic control, management of household appliances or personal medical devices and the working world. Cyberspace is the new battlefield and geopolitical competition of the 21st century. This new dimension can make political imbalances, which dominate international relations, uniform, placing subjects of the most diverse nature on the chessboard: single individuals, non-state actors and States. These act on an almost equal playing field, thus eliminating any form of asymmetry. In fact, in every act of war, the physicality of those who act on land, sea, air or space makes the actors easily identifiable, just as the borders of the belligerent state are also easily identifiable. The same does not happen in cyberspace, where, due to its intrinsic digitised nature, it is very complex not only to impute the action in time to one or more specific subjects and/or to a State, but also to understand the reason for the attack and its objectives and, above all, to avoid that those who have acted can easily escape from any legal, political, diplomatic, economic and military responsibility (Mele, 2010).

Cyberspace, if on the one hand, it contains in itself the potential to allow an unprecedented development of economic and productive activities of commerce, of the efficiency of public administrations and the exercise of people's rights in unprecedented forms, on the other hand, it is an opportunity for the new forms of threat to productive activities, to the enjoyment of citizens' freedoms, to the action of public authorities and of the States themselves to manifest themselves (Iaselli, 2020). The threat (NSFSCS, 2013), although it relates to the intangible world of cyberspace, is very concrete and is becoming increasingly prominent in governments' concerns. The security of cyberspace has reached a strategic connotation comparable to that of the protection of physical space, so much so that it represents one of the major concerns and sources of investment by major global players, given that the Internet is now understood as the critical infrastructure par

excellence. States, therefore, are now called upon to devise, plan and implement defence measures, as they have always done to defend real space.

4. From the digital revolution to the criminal revolution

If the crime has accompanied humanity since the dawn of its evolutionary history, the digital revolution has also represented a sort of criminal revolution: after the first moments of uncertainty, information technologies have confirmed themselves as fertile ground, in which the new expressions of crime organized occupy an ever greater space, directly proportional to the computerization process that is underway (Lorusso, 2011). The speed of the Internet, capable of moving large masses of information from one part of the world to another in fractions of a second, has been recognized as a winning weapon by criminal organizations, which have not been slow to use the 'electronic highways' to make run their own money, coming from the most disparate illicit operations. Criminal organizations need to ensure a flow of financial resources that must necessarily be reinvested. These resources are functional to the corruption of public officials. The Internet lends itself well to these purposes, both by allowing the perpetration of computer fraud and by promoting cyber-laundering, facilitating the exchange of information and thus avoiding dangerous communication dynamics represented by direct contact (Cadoppi et al., 2019; Richet, 2013).

Therefore, technological progress has been accompanied by a constant and unstoppable growth of the activities carried out by cybercriminals, whose goal is no longer notoriety, but the implementation of a real business model different from the past, as it is organized, as stable as possible and able to survive over time. Today, we are in the presence of real criminal organizations, managed by subjects motivated by important and lasting profits, deriving, for example, from the sale of personal data and cloned credit cards or from cyber-extortion by ransomware (Cadoppi et al., 2019). Cybercrime has therefore taken on the contours of a real underground economy (a phenomenon that includes not only illegal activities, but also undeclared income, deriving from the production and sale of goods and services and monetary transactions and all legal economic activities, but not declared, to which the tax authorities could apply a taxable amount), globalized and efficient, where illegally stolen goods and fraudulent services are sold and purchased and where the estimated turnover is measurable in millions of dollars (Europol, 2011).

With the development of information technologies, therefore, we have witnessed digitization of organized crime which is continuously looking for uncontrolled places in which to conduct its criminal business with confidence. The Net undoubtedly represents a 'free zone', as it can provide sufficient guarantees of security and anonymity. The spatial multidimensionality of the Net is perfectly suited to this business model and the effort to raise illicit profits within an acceptable degree of risk (Santoro, 2011).

5. Transnational cybercrime

The globalization of information, generated by the advent of new technologies, has allowed the creation of a free market without borders in which cybercrime takes on transnational backgrounds and reflections (Foggetti, 2004). Cybercrime has therefore become globalized. The process of globalization, on the one hand, has contributed to enhancing the opportunities for activities worthy of protection, on the other hand, it has facilitated the development and sophistication of criminal groups operating on transnational markets. The numerous opportunities created by globalization, such as the abolition of borders, the creation of new business, new markets and the provision of new, more powerful and sophisticated means of communication and exchange, have been fully exploited by criminal groups, representing the ideal preconditions for the carrying out of criminal activities on a large scale.

Therefore, we are witnessing the birth of a new crime, which escapes traditional models and aspires to control global economic trafficking, allocating part of the lucrative proceeds of this activity to the financing of further illicit trafficking, in a growing and negative spiral for the contemporary economy (Santoro, 2011). The new modern economy of globalization and the Internet is essentially based on five pillars of crime: 1) financial transactions, which represent the recycling of all other forms of crime; 2) trade-in weapons and toxic-noxious materials; 3) trade-in living organs dissected for transplants; 4) trade-in natural and synthetic drugs, pollution and plundering of the environment; 5) and cybercrime. All the forms of crime listed have a single glue that unifies them and merges them with the circuits of the economy: the finance (Santoro, 2011). Transnational crime, therefore, represents a serious threat to the economic and financial systems of all States, especially as a result of the current inability of contemporary society to deal with new criminal phenomena, due not so much to new forms of crime, but more to the ineffectiveness of the remedies proposed by some parties.

The cyber groups, which operate in the 'transnational network', have peculiar characteristics, such as flexibility and a high level of organization, which contribute to complicating the work of the investigative authorities and of all those bodies and institutions, which seek to prevent and combat computer crimes. Cyber groups tend to 'maximise' the opportunities offered by new communication technologies and profits (opportunities for crime and enrichment) and to 'minimise' the risk of being identified, arrested, convicted and to have seized the proceeds of their criminal activities. These two factors change very rapidly as a function of variables that are difficult to manage, especially if their evaluation must be carried out on wide and complex international scenarios (Ambos, 2015). The lack of homogeneity of criminal laws also contributes to making the real prosecution of cybercrime even more complex, because of which the same conduct can assume, depending on the legal system considered, different qualifications.

6. Conclusions

While the spread of information and communication technologies in modern society has contributed to improving the performance of economic and civil systems, on the other hand, it has exposed democracies to a relatively new type of crime, the cybercrime, which in recent years it has affected companies, public administrations, critical infrastructures and private users, causing large-scale damage. This new criminal form was born, grew and rooted at the same time as the development of the Net. It is a criminal manifestation, which is not limited to national borders but takes on a transnational connotation, which guarantees agents a context of virtual impunity. Given the contradictory and heterogeneous international legal framework, the concern is that many States become potential grey areas, from which cyber criminals could operate without an adequate State response in terms of prevention, sanctions, containment, and enforcement.

Fighting the phenomenon of cybercrime becomes a particularly complex operation due to the jurisdictional problems that arise at a national and international level. The traditional forms of jurisdiction are based on the concept of 'border' and the laws on that of territorial sovereignty. In cases of a cybercrime having a transnational scope, the identification of the *locus commissi delicti* is difficult. This entails the loss of a fundamental element of the criminal system of most legal systems, which are based on the principle of territoriality as the main criterion in the definition of the judge competent to know the illegal fact. Considering that cybercrime has branched into a transnational dimension, we understand how the struggle to combat this phenomenon must take on the same character; this requires first of all the circulation of information and greater cooperation between the investigative authorities of the individual countries. It becomes imperative to prepare strategies, such as judicial collaboration and to have a common regulatory system as necessary preconditions to counter this type of criminal manifestation. In such a complex context, we must abandon the purely nationalistic perspective of the repression of cybercrime, in favour of an approach that goes beyond national limits in the implementation of the law. The sovereignty of the states, in the context of the repression of cybercrime, is identified as an insurmountable obstacle in the realization of a supranational union of law. Therefore, to put legal practitioners in the real conditions to suppress transnational cybercrime, a 'globalization of justice' is necessary.

Conflict of interest
The authors declare no conflicts of interest.

Authors' contribution
Both authors contributed equally to the conception and writing of the manuscript.

References

Ambos, K. (2015). International criminal responsibility in cyberspace. In *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing.

Balsano, A. M. & Del Monte, L. (2013). Il diritto internazionale di fronte al cyberspace. In Osservatorio per la sicurezza nazionale (Eds.), *Cyberworld. Capire, proteggersi e capire gli attacchi in rete*. Milano: Hoepli.

Cadoppi, A., Canestrari, S., Manna, A., & Papa, M. (2019). *Cybercrime*. Vicenza: UTET Giuridica.

Europol Press Release (2011). Cybercrime as a business: The digital underground economy. Available at https://www.europol.europa.eu/newsroom/news/cybercrime-business-digital-underground-economy

Faga, H. P. (2017). The implications of transnational cyber threats in international humanitarian law: analysing the distinction between cybercrime, cyber-attack, and cyber warfare in the 21st century. *Baltic Journal of Law & Politics*, *10*(1), 1-34.

Floridi, L. (2012). *La rivoluzione dell'informazione*. Torino: Codice Edizioni.

Foggetti, N. (2004). Ipotesi di criminalità informatica transnazionale: profili di diritto applicabile al caso concreto. Problematiche attuali ed eventuali prospettive future. In AA.VV., *Diritto e società dell'informazione. Riflessioni su informatica giuridica e diritto dell'informatica.* Milano: Nyberg Edizioni.

Iaselli, M. (2020). *Investigazioni digitali*. Milano: Giuffrè.

Levy, P. (1997). *Il virtuale*. Milano: Raffaello Cortina Editore, pp. 9-14.

Lorusso, P. (2011). *L'insicurezza dell'era digitale. Tra cybercrimes e nuove frontiere dell'investigazione*. Milano: Franco Angeli.

Martino, L. (2018). La quinta dimensione della conflittualità. L'ascesa del cyberspazio ei suoi effetti sulla politica internazionale. *Politica & Società*, *7*(1), 61-76.

Mele, S. (2010). Privacy ed equilibri strategici nel cyber-spazio. *Diritto, economia e tecnologie della privacy*, *1*.

Pansa, A. (2004). *Cybercrime: conferenza internazionale. La Convenzione del Consiglio d'Europa sulla Criminalità Informatica.* Milano: Giuffrè.

National strategic framework for the security of cyber space (2013). Retrieved from https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf

Rapetto, U., & Di Nunzio, R. (2001). *Le nuove guerre: dalla cyberwar ai black bloc, dal sabotaggio mediatico a Bin Laden* (Vol. 11). Milano: Rizzoli.

Richet, J. L. (2013). *Laundering Money Online: a review of cybercriminals' methods*. Available at https://arxiv.org/abs/1310.2368.

Santoro, F. (2011). *Cooperazione internazionale in materia di criminalità informatica*. Roma: Aracne Editrice.

Teti, A. (2018). Cyber espionage e cyber counterintelligence: spionaggio e controspionaggio cibernetico (Vol. 9). Catanzaro: Rubbettino Editore.

Teti, A., & Caligiuri, M. (2015). *Open source intelligence & cyberspace: la nuova frontiera della conoscenza*. Rubbettino.

We are Social (2019). Report available at https://www.slideshare.net/wearesocial/digital-in-2018-global-overview-86860338.