Understanding Cybercrime and the Phenomenon of "Broutage" (Grazing) For a Media Education of Pupils and Students in Côte d'Ivoire

Okon Marguerite KOFFI – DJAH1, Benoît Kouakou Oi KOUAKOU2
1,2Department of Information and Communication Sciences, UFR Information, Communication and Arts (UFRICA)
Felix Houphouet-Boigny University of Abidjan

ABSTRACT: This article analyzes some understanding outlines of cybercrime considering its complexity and its practice by the youth population in Côte d'Ivoire for media education. On the basis of conventions, guides and scientific publications on the phenomenon, a thematic content analysis was conducted in order to identify the axes that structure the study in response to the research objective. This problematic is based on the socio-ecological model of Sallis and Owen (1998). According to the Preamble of the Council of Europe's Convention on Cybercrime, known as the "Budapest Convention" of November 23, 2001, which entered into force on July 1, 2004, cybercrime is crime in cyberspace. In the absence of a legal definition of the phenomenon, there is confusion between crimes germane to cybercrime and cybercrime itself. The Internet, a channel of cyberspace, is presented as a web, a mesh on a planetary scale that limits the control mechanisms and reveals the difficulties of quantifying the phenomenon. Through a vicarious learning among young people in Côte d'Ivoire, cybercrime colloquially called "broutage" (grazing) is a social malaise, despite the response of the Ivorian state. The use of ICTs requires education to make each user responsible for understanding, using, defending and enjoying them, because the media world is experiencing an unprecedented shock.

KEYWORDS: Communication, cybercrime, media education, ICTs, youth.

INTRODUCTION
Most of the scientific literature on cybercrime opens with an attempt at a definition. The term remains difficult to conceptualize, as it is not the subject of any legal definition. Cybercrime is a protean reality which is still unclear and undefined (Robert, 2014). The necessary evolution must take into account the lessons of comparative law, the expectations of public opinion, actors and victims, as well as the requirements concerning the protection of fundamental freedoms. This choice of the legislators has led the doctrine to multiply the definitions of this term, thus contributing to the complexity of legal analyses. One must consider the conception of cybercrime contained in the Preamble of the Council of Europe's Convention on Cybercrime, known as "The Budapest Convention" of November 23, 2001, which entered into force on July 1, 2004. According to the provisions of the Preamble, cybercrime is crime in cyberspace1. The absence of a legal definition of cybercrime, as mentioned above, is a source of confusion regarding the fields of thinking and analysis or regarding the appropriate terminology. These confusions led us to analyze the understanding outlines of the phenomenon in its general sense and its practice in a precise context by a defined target. Undoubtedly, the practice of cybercrime by young people in Côte d'Ivoire reflects a social malaise, hence the need for media education.
The study is based on the socio-ecological model, which we believe, is more robust and fruitful for the comprehensive analysis of the social, technological, and organizational interactions that shape the digital risk environment. Conceiving the cybercrime ecosystem as the convergence of criminals, and security and organizational actors following unique respective rationalities will help to overcome the confusion created by the complexity of this new criminal architecture. This is done by simultaneously taking

Understanding Cybercrime and the Phenomenon of "Broutage" (Grazing) For a Media Education of Pupils and Students in Côte d'Ivoire

into account the cooperative, competitive and predatory relationships that characterize this ecosystem. Based on its onion-like structure, this ecosystem considers knowledge, motivation, and capacity building, in which change occurs (Sallis and Owen, 1998).

A thematic content analysis was conducted from the conventions, guides, and scientific publications on cybercrime in order to identify the axes that structure the study in response to the research objective.

I. CYBERCRIME AND CRIMES RELATED TO IT: A CONFUSION BETWEEN THEM

In the absence of a commonly accepted definition of crime in cyberspace, the terms cybercrime, computer-related crime or high-tech crime are often used interchangeably.

In the classification of cybercriminal offences, it is common to see that these infringements are grouped according to whether they concern property, people or computer systems themselves (Quemener, 2010). This is why the laws against cybercrime must also cover these particular areas. However, their enforcement from one State to another does not follow the traditional nomenclature of offences. A distinction related to legal terms is then necessary.

1. Cybercrime and computer-related crime

Totty and Hardcastle (1986, p. 169) posit that computer-related crime covers crimes in which a computer has played an active rather than a passive role. Hacking includes not only fraudulent actions mainly on the computer system itself (software) but also the theft of computer data and works. According to Article 7 of the Budapest Convention, computer forgery and fraud are considered computer offences. These practices are parts of several offences. As a matter of fact, hacking in itself is not an isolated practice. It is the beginning of the execution of acts such as illegal interception. It is also related to computer forgery, the offence to which it is closer in terms of constituent acts.

Some authors put several offences together under the term computer-related crime. This is the case of the Council of Europe, which lists in its Final Activity Report on computer-related crime the offences that European law must punish. These are: fraud, forgery, sabotage, unauthorized reproduction of a protected computer program, espionage, alteration of computer programs and data and damage to data and programs.

MARTIN (1999, p. 13) thus defines computer-related crime as any illegal action in which a computer is the instrument or object of the crime; any crime whose means or purpose is to influence the function of a computer; any intentional act, associated in one way or another with computer technology, in which a victim has suffered or could have suffered harm and in which the perpetrator has made or could have made a profit.

Cybercrime, in its strictest definition, refers to all offences committed with the help of or against a computer system connected to telecommunications network. It has a wider scope since, in addition to offences against computer property that can be committed via the Internet, computer-related crime and cybercrime have a common branch when computer offences are committed through the use of the telecommunications network. But not every computer crime is committed by means of a telecommunication network. And not every offence committed by means of a telecommunication network is systematically a computer offence. This confusion of the object of cybercrime in the legal sense of the term is evident from one border to another.

Outside of European borders, the United States Department of Justice defines cybercrime as “any violations of criminal law that involve a knowledge of computer technology for their perpetration” (Tano-Bian, 2016). The author however believes that the American conception of cybercrime is questionable because it does not take into account all potential cybercriminals including the fence or accomplice to cybercriminal acts. As for the Swiss Federal Office of Police, it considers cybercrime as the set of new forms of crime specifically linked to information technologies, and known crimes that are committed with the help of computers rather than with conventional means.

2. Cybercrime and high-tech crime: international dimensions of anonymous communications

Basic pieces of equipment like hardware, software and Internet access are enough to commit cybercrime. To limit the risk of identification, most cybercriminals do not subscribe to the Internet. They rather prefer using free access (without registration with checking procedures).

“Wi-Fi hacking” is a classic method of gaining network access. It consists in scanning wireless networks using one's car in search of access. The most common means of network access used by cybercriminals to gain relatively anonymous network access are

---

Understanding Cybercrime and the Phenomenon of "Broutage" (Grazing) For a Media Education of Pupils and Students in Côte d'Ivoire

public Internet access terminals, free (wireless) networks, hacked networks, and prepaid services without registration (Telecommunications Development Sector Report, 2012).

Cybercriminals use fake email addresses as a means to hide their identity. Many providers offer free e-mail accounts. However, personal information, when requested, is not always verified. It is therefore possible to create e-mail addresses without revealing your identity. The anonymous address has an advantage: it allows, for instance, an Internet user to join a political discussion group anonymously. On the one hand, anonymous communication can encourage anti-social behavior; on the other, it gives Internet users greater freedom. It is clearly necessary, in view of all the traces left by users on the Internet, to prevent, through legislative instruments, the profiling of activities on the network.

Indeed, ICTs have a considerable advantage by making certain processes automatable. Automation has several important consequences: it increases the speed of processes, their scope and impact and, finally, it helps to limit human intervention. Through automation, cybercriminals can intensify their activities: sending spam emails, hacking attempts, etc. The distributed nature of the network, as well as the availability of some Internet services, which creates uncertainty about the origin, is an obstacle to identifying cybercriminals.

These apparent manifestations of cybercrime interact with high-tech crime. According to Martin (2001), high-tech crime is the crime that includes all the illegal acts related to computers and telecommunications, both in terms of hardware and software. It concerns computer crime as such and forgery, cloning of electronic components capable of creating malfunctions in information and telecommunications systems or allowing fraudulent use. From this point of view, high-tech crime can cover two categories:

- Offences related to computer systems that are not connected to telecommunication networks,
- Offences related to computer systems that are connected to telecommunication networks.

Only the second category of offences committed via telecommunications networks are considered as cybercrime according to the definition given by the Budapest Convention. However, not all high-tech crimes are cybercrime. How then can the control mechanisms of cyberspace be analyzed?

II. LIMITATIONS OF INTERNET CONTROL MECHANISMS AND THE ISSUE OF QUANTIFYING CYBERCRIME

1. Limitations of control mechanism

A report by the Telecommunication Development (2012) states that all mass communication networks, from telephone networks for voice communication to Internet networks, require central management and technical standards that ensure good operability. Ongoing studies regarding Internet governance tend to indicate that this network is no different from other national or even transnational communication infrastructures. The Internet too must be governed by laws. However, it should be emphasized that the Internet is not in space, it is space (Levi, 1995, p. 17). Thanks to the interconnection of numerous premises, the Internet appears as a web, a mesh on a planetary scale. This vast so-called distributed architecture explains its decentralized organization. What is there between a phenomenon that ignores borders, and entities that only exist and have jurisdiction within given borders? Its regulation is already affected by a pathogenic law (Viviany, 1996, p. 226). On this point, doctrine as well as governments agree to recognize the gap between the fiction of the omnipresent State and the reality of the network because of its transnational feature. The Internet is not a space where the heterogeneous group of Internet users organize themselves hierarchically in respect of a State at the top of the pyramid.

Originally, the Internet was set up as a military network based on a decentralized architecture in order to keep the main functionality intact and operational, even in case of an attack on certain network elements. And as Bechillon (1997, p. 10) would say the object of any rule resides from the outset in the squaring of human conduct, in this sort of measure that humanity gives itself to regulate its relational affairs. With its infrastructure, the Internet then resists any external attempt to taking control of it. In the initial specifications, it was not foreseen to facilitate investigations for infringement nor to prevent attacks from inside the network.

Furthermore, the ubiquity of the Internet in the civilian sector remains a problem. The report by the Telecommunication Development notes that this evolution from the military to the civilian sector is accompanied by an evolution in the demand for control instruments. Because the network is based on protocols designed for military purposes, such instruments do not exist at a central level and are difficult to implement a posteriori without a major rethink of the overall design. The lack of these control instruments makes it very difficult to investigate cybercrime.

Due to the lack of control instruments, Internet users can bypass filtering techniques by using encrypted anonymous communication services. Normally, it is impossible to connect to Internet sites with illegal content if the Internet Service Providers (ISPs) have blocked access to them. Yet, by using an anonymous communication server that encrypts transfers between Internet
Understanding Cybercrime and the Phenomenon of "Broutage" (Grazing) For a Media Education of Pupils and Students in Côte d'Ivoire

users and the central server, it is possible to bypass the blocking of contents. Indeed, since the requests are sent in encrypted form, the ISPs are not able to read them and, consequently, to block them.

2. Quantification problem

Never before has a criminal phenomenon been the subject of so many peremptory assertions. These assertions also coming from official international organizations are about the importance of the phenomenon and the harm it causes. However, if all the actors agree on this importance and seriousness, the sources of information seem fragmented and approximate. In all countries, the quantification of the phenomenon comes up against comparable difficulties. The apprehension of cybercrime must first be based on the legal definition of offences (Report of the Inter-ministerial Working Group on the Fight against Cybercrime, 2014).

Thus, the first challenge is for the courts to base their statistical system on the concept of offence, which is not possible with existing enforcements. Yet, the legal definition of offences is, in most cases, insufficient to take into account cybercrime when it is only the means to commit an ordinary offence: the law does not include any distinctive element regarding their perpetration by means of an information system. Therefore, the second challenge for police and judicial statistical systems is to consider, even when the law is silent, the specific modus operandi4 of cybercrime, when it exists; this can only be done on the basis of the findings of investigators. In such a context where the State cannot be the main guarantor of digital security, it is not surprising that it does not keep any usable records. In the field of cybercrime, Wall (2015) supports that no one can claim to be exhaustive or even hope to be exhaustive. The State intervenes essentially on the repressive side since it does not have a monopoly on a reliable source of information. The private sector of protection solution sales (anti-phishing or anti-virus software for example) is in a better position, but its counting possibilities remain partial. The author proposes to compensate for the shortcomings of police counts with general population victimization surveys and with national or local instruments that ask people about crimes they have allegedly experienced over a given period. How do young people in Côte d'Ivoire appropriate the practice of cybercrime? What is the response from the Ivorian state?

III. "BROUTAGE" (GRAZING), A VICARIOUS LEARNING PROCESS AMONG YOUNG PEOPLE: WHAT IS THE IVORIAN STATE'S RESPONSE?

1. Origin and explanatory factors

Since the onset of the military and political crises in Côte d'Ivoire, Ivorian youth have been characterized by exponential delinquency, as many of them have become adept at the art of cybercrime colloquially known as "broutage" (grazing). The phenomenon has taken over from the practices initiated by female students in the early 2000s who easily obtained money transfers from their European correspondents (Yaya, 2017). The cultural movement called the "coupé décalé", born out of swindling, is said to be at the origin of the dance of the “brouteurs” (grazers), and has participated in the development of "broutage" in Côte d'Ivoire (Gbadamassi, 2003). Adored and courted, many of the "brouteurs" recruit other young people because they succeed in seducing them through their dandyism and their "travaillement". In Ivorian slang called Nouchi, "couper" means to swindle and "décaler" means to run away (Kohlhagen, 2005). Hence the expression "couper l'herbe sous les pieds" (to cut the grass under the foot) gives all its meaning to deception. These youth criminal organizations carry out the most sophisticated and targeted attacks. Individuals are paying a heavy price for this expansion of "broutage." This phenomenon has not only taken on a significant proportion in the world but has also taken on particular forms in Africa ("Yahoooboy" in Nigeria; "feymens" in Cameroon; "gays mans" in Benin; “brouteurs” in Côte d'Ivoire). It is an appropriation or even an "Ivorianization" of the Nigerian-style scam (Adou, 2022), and therefore a new, more astute form of criminality called "broutage 3G." This terminology refers to the adage that the sheep grazes everywhere. In other words, commercial, banking, and financial transactions taking place on the web and across the cyber world provide multiple criminal opportunities for these "brouteurs" (Akadjé et al, 2017). This criminal activity highlights the mechanism of vicarious learning among youth. It is a "contagious" phenomenon. The “brouteurs” are organized networks with leaders who recruit. They roam cybercafés, their favorite working places.

General explanatory factors stem from the precarious socio-economic context, the development and the ecosystem of the Internet and ICTs and the weakness of the legal framework for ICTs. Like any social phenomenon, the explanatory causes of cybercrime in the youth population are diverse and varied: the pressure of unemployment of young graduates lured by easy gain,

4 Latin expression formed from "modus" (way) and "operandi" (to operate), it designates the way of realizing and building something.
5 Colloquial word of the local slang Nouchi: the “brouteurs” are prodigal children who ostensibly redistribute in bars and night clubs the sums of money they have amassed.
Understanding Cybercrime and the Phenomenon of "Broutage" (Grazing) For a Media Education of Pupils and Students in Côte d'Ivoire

the school crisis, the lack of parental authority, etc. have as an inevitable consequence the loss of values that are essential to education, development and citizenship of young people.

2. Ideology and modus operandi
The practice is supported by a particular mechanism that stimulates its ideology and modus operandi. The practice is also based on an argument structured around the notion of social justice and the belief in a European land of plenty. On the internet, they construct in parallel the social and professional “black mask” of the “Brouteur” by modulating themselves in the virile standards of extortion and power of control. According to their ideology, the time has come to pay back the colonial debt. According to Wintjens (2020), the colonial debt is an ancestral robbery, a legalized plunder. The economic implications of debts imposed on colonized States have led to social disasters that are still observed today in many countries. In response, the brouteurs’ favorite targets are the "peaux grattées" (Ivorian slang for white Europeans). They are supposed to pay this debt. The modus operandi is then varied and innovative.

The Nigerian method consists in sending emails to addresses previously retrieved from sites through the use of adapted software, with content that arouses empathy for scams of all kinds.

Asking for help: here, religions and companies are victims. Frauds create Internet sites pretending to be religious associations seeking funding for the construction and renovation of religious buildings in order to swindle potential donors.

Romance scam: With this practice, the “brouteur” uses the bond of trust with male or female victims from Europe to lend himself to a certain erotic practice in front of his webcam. This is followed by a real blackmail in terms of financial gain to which the victims succumb, devastated by the shame and fearing to kill themselves, if these images are published worldwide. The new trend consists in an infiltration in the networks of online pimps. The story of the Ivorian "Yoyo la gazelle" is creating the buzz of social networks. A fearsome young girl who has emptied the accounts of her suitors.

Ritualistic method: The practice of black magic includes mystical processes carried out in the shadows. For Bazare et al. (2017), all cybercriminals engage in this practice but for different purposes. Most of them want to bewitch their target in order to annihilate any will of resistance and refusal of the potential victim. For others, in their understanding, these mystical rituals help them to escape the police and justice.

Bazare et al. (op. cit.) identify four categories related to the profile of cybercriminals. The Novices constitute the first category. They are young males between 13 and 17 years old. Most of them are high school students and learning begins with this category. The second category is composed of Amateurs, aged between 18 and 23. They know about computer tools and they always work under the supervision of older youth, masters of the domain. The third category includes the Professionals, aged between 24 and 29. They are students and they are able to penetrate the security zones of the most protected networks, unknown to all, except ICT experts. And finally, the Experts form the last category. They are between 30 and 34 years old. They are passionate about computers and are generally called "Hackers."

The search for easy money seems to be the only concern of the majority of these crooks coming from disadvantaged backgrounds (Gueu, 2018).

3. Response from the Ivorian State
Securing cyberspace is a requirement to support digital transformation. To counter cyberattacks that have long tarnished the image of Côte d'Ivoire, the government created in 2011 the Plateforme de lutte contre la cybercriminalité or PLCC (Platform for Combating Cybercrime). A commando 2.0 that tracks threats of publication of sexual images and sexual harassment on social networks (Facebook, Instagram, Twitter, Snapchat, WhatsApp), fraud on electronic transactions, fraudulent use of identification elements of natural persons, damage to image and honor, online scams, etc.

According to the Director of Computing and Technological Traces of the Ministry of the Interior and Security, the Platform registers an average of 4,500 to 5,000 complaints per year. Composed of investigators, engineers and technicians in the fight against cybercrime, the PLCC carries out judicial investigations and organizes the tracking down of cybercriminals. The intensification of the fight and the reinforcement of the means deployed have helped the structure to increase the tracking. Thus, the number of cases taken in charge is clearly increasing, 5,000 cases in 2021, against 2408 complaints in 2017 and 150 in 2011. The resolution rate of cybercrimes is 50%. The Ivorian cyberspace, once undermined and avoided like the plague, tends to be cleaned up. In addition to tracking and repression, the PLCC is also an instrument of awareness. It educates more than 25,000 students a year about the evils of cybercrime. Experts advise them, for example, to be careful on social networks and warn them against publishing fake news. After the creation of the Platform in 2011, the government strengthened in 2013 the legal arsenal by adopting the law No. 2013-451 of 19 June 2013 on the fight against cybercrime. The fight against cybercrime will be further strengthened in March
Understanding Cybercrime and the Phenomenon of "Broutage" (Grazing) For a Media Education of Pupils and Students in Côte d'Ivoire

2019 with the ratification of the Budapest Convention on Cybercrime of the Council of Europe. This convention allows Côte d'Ivoire to benefit from international collaboration in its fight, for greater effectiveness (CICG, 2022). Beyond alternative messages and repression that are closer to the real issues, it is imperative to oppose this vicarious learning with media education for the autonomy of young people.

IV. OF THE NECESSITY OF MEDIA EDUCATION FOR THE AUTONOMY OF PUPILS AND STUDENTS

The “brouteurs” are brilliant at social engineering. Philippe Breton and Serges Proulx (2012) find that, depending on the contexts of analysis and the theoretical frameworks mobilized, the notion of usage, which is otherwise quite complex, refers to a continuum of definitions, ranging from the pole of simple "adoption" (purchase, consumption, expression of a social demand with respect to an industrial offer) to the pole of "appropriation." In the latter case, they consider that we can speak of “appropriation” when three social conditions are met. First, the user must demonstrate a minimum of technical and cognitive mastery of the technical object. Secondly, this mastery must be integrated in a significant and creative way into the daily practices of usage. Thirdly, appropriation opens up possibilities for misuses, bypasses, reinventions or even direct participation of users in the design of innovations.

The usage of the Internet for fraudulent purposes by a large segment of the youth population has extremely harmful consequences on the country’s image, on its economy and education, since cybercriminals are young people. The current evolution of ICTs increases crucial societal issues. Their usage requires more than ever an education aiming at making each user responsible to understand them, use them, defend themselves from them and take advantage of them, because the world of the media undergoes an unprecedented shock. This learning process draws its legitimacy from the discourses on the protection of children and young people and on education for citizenship. Media education is positioned within a triangulation between school, media and democracy. To this end, for Frau-Meigs (2011), Chomsky (2012), media education poses a major issue: its capacity to prepare the learner to face a complex and changing media universe. This produces concrete knowledge aimed at developing not only a praxis of critical thinking in learners but also a plethora of cognitive, technical, behavioral and ethical skills.

Indeed, each learner receives and understands a media reality according to his or her own experience, beliefs, etc. There are, therefore, biases that have an influence on their reception, dissemination and judgment. These are: the anchoring effect and the weight of our a priori ideas, the cost of abandoning our beliefs (Gauvrit, 2019). For the European Commission (1989), media literacy is the ability to access the media, to understand and critically appreciate different aspects of the media, their contents and to communicate in various contexts. Learners should be introduced to the structures, mechanisms and messages of the media; in particular, they should develop an independent capacity to think critically about media content.

Vize (2010) supports that media do not present reality, they represent it. Thus for Charauadeau (2005), if the media are a mirror, they are only a distorting mirror. Each of the media has its own way to testify of an amplified, simplified, stereotyped parcel of the world. Consequently, in the context of the construction of a free and responsible citizenship, it is only those of the publics that possess the keys of a critical and distanced reading that will be able to understand "how", "by whom" and "why" the media elaborate the messages that they broadcast, and that will be able to avoid consuming ethically, politically and culturally questionable media contents.

Thus, for these authors, it is important to use a critical spirit to deconstruct any media message or content. To deconstruct a media message means to decipher the codes of representation, as one learns to read and write, not to be illiterate.

DISCUSSION AND CONCLUSION

Cybercrime is a broad and artificial concept with a significant dimension in terms of the variety of illicit acts committed, its internationalized nature, and the damage caused to states, businesses and individuals (UNODC, 2013). It is clear that the Internet poses new and multiple problems for the law. The network is the result of the deregulation of the telecommunications sector, which introduces a certain normative autonomy of actors. States now partially share their sovereignty through a negotiated law that is characterized by its relativity, its heterogeneity and its fluidity (Diebolt, 2000). Notwithstanding the apologetic speeches on the messianic power of the Internet, the fact is that this tool remains nowadays a criminogenic tool.

The appropriation of the practice of cybercrime, particularly by young people in Côte d'Ivoire, suggests a North/South dialogue between two parties who evolve in a different digital environment, one connected from a private space and the other from a public space. This Ivorian-style open space has a theatrical dimension (Yaya, Op.cit).
Understanding Cybercrime and the Phenomenon of "Broutage" (Grazing) For a Media Education of Pupils and Students in Côte d'Ivoire

The gradual constitution of a class of citizens who are more informed and educated, critical, skeptical and reflective about the processes of production, dissemination and reception of media information and media culture would be an asset. It is assumed that this could contribute to a strengthening of democratic foundations and a mitigation of inequalities and social injustices (Landry and Basque, 2015).

The fear of innovation or the hasty and/or misguided adoption of ICTs is the result of a lack of anticipation with regard to educational or security realities. However, in this digital age, it is unthinkable that it can be done without ICTs, even though it is problematic. This is the basis for the place to be given to media education in the construction of an African information society in order to meet this social, cultural, economic and political challenge.

REFERENCES
3) Bamba, I. and Bazare, N.R., 2016. Festive practices of “grazers” in CI: between ritualization of the party and social categorization of cybercriminals

There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non Commercial 4.0 International (CC BY-NC 4.0) (https://creativecommons.org/licenses/by-nc/4.0/), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.