IADIS International Journal on Computer Science and Information Systems
Vol. 18, No. 2, pp. 35-57
ISSN: 1646-3692

STUDY OF CYBER AGGRESSION FACTORS AMONG YOUNG CONGOLESE STUDENTS

Efrem Mbaki Luzayisu[1] and Jean-Pierre Zamwangana Tungu[2]
[1]*Professor at University of Kinshasa and at Catholic University of Congo, Congo*
[2]*PhD in Demography and Independent Researcher*

ABSTRACT

For several years now, the literature has been reporting an increase in aggression via the Internet among young people living in developed countries. Despite the financial and technical difficulties due to the situation in the country, young Congolese are also very open to ICTs and fun of all kinds of online applications that make them vulnerable to cyber-attacks. In this context, this study aims to examine the prevalence and factors affecting online aggression in Congolese academia. Indeed, with a field survey of 1500 students, we found that students who engage in high-risk online behaviors, such as sharing the Internet connection with others, posting content online, or dating virtual friends, are among those who have a higher probability of being victims and/or perpetrators of online assault. Based on the findings we formulated some recommendations that can help reduce the prevalence of cyberaggression.

KEYWORDS

Cyberaggression, Digital Behavior Risk, Hyperconnectivity, Parental Control on Student Internet Use, Cyberbullying, Self-Esteem, University Students, Democratic Republic of the Congo (DRC)

1. INTRODUCTION

The topic of cyber aggression that we address in this document is not new. The literature shows that it has received increasing attention over the last two decades (Finkelhor et al., 2000; Hashima & Finkelhor, 1999; Mitchell, 2003). While recognizing that online aggression does not only concern young Internet users, the interest in these attacks can be explained in particular by the increasingly early use of digital tools, but also by their harmful impact on psychological development, well-being and school performance.

Nowadays, cyberaggression or online aggression is gaining more and more ground, particularly among children, teenagers and young adults (Bauman, 2009; Bauman & Baldasare, 2015; Blaya, 2015; UNICEF, 2019). This is a vulnerable and Internet-avid population, “digital natives” or “digital children”, as they are sometimes called. Born with a mouse in hand, young people find it difficult to separate themselves from the Internet, which is an integral part of their lives. This is not just about children in Western countries; those of the countries of the South are also involved. But browsing the Internet also exposes them to attacks of all kinds. Why are these young people victims and/or perpetrators of online aggression? Is it because of their hyperconnectivity? Is this a consequence of a lack of awareness of the dangers that the Internet can represent? Or is this the expression of new forms of violence that find favorable ground among young people? The theories on the subject are juxtaposed and overlapped to try to understand this social phenomenon.

Two types of studies are currently of interest to researchers working on attacks on the Internet. On the one hand, methodological approaches are developing to better define and better assess online aggression among young people (Baldwin et al., 2015; Bauman & Baldasare, 2015; Blaya, 2011; Menesini et al., 2012; Yusuf et al., 2021); and on the other hand, more and more studies are moving towards the identification, if not the causes, of the risk factors at the origin of this online phenomenon (Blaya, 2013; Les Études du Center Jean Gol, 2017; Macilotti, 2019).

The present study aimed to evaluate the prevalence of cyberaggression among university/college students in the Democratic Republic of the Congo (DRC) and examine risk factors associated with cyberaggression among these students. The paper is organized around seven sections. In the first section, we have summarized the problem statement of the study by specifying why we decided to conduct it. In the second section we have summarized our conceptual framework based on a review of literature around online aggression towards the World. We have described our materials and methods used to analyze data and the study participants in the third section before opening a brief parenthesis about general information on cyberaggression in the fourth section. Thus, the fifth section presents the main findings. Those results are briefly discussed in the sixth and last section, where study limitations and recommendations are also presented.

2. PROBLEM STATEMENT

Attacks on the Internet, mobile phones and other digital platforms, such as Facebook, SnapChat, Instagram, Pinterest, WhatsApp, Twitter and Tiktok, are becoming a worrying societal phenomenon, especially when they affect children, adolescents and young adults. They often take the form of insults, threats and other forms of harassment towards their victims and they can have various mental, educational and psychosocial repercussions (European Parliament, 2016; Macilotti, 2019; UNICEF, n.d.; Yusuf et al., 2021). On the school level, for example, some scholars (Even, 2019; Yusuf et al., 2021) mention, among other things, school and psychosomatic disorders which considerably affect the development of adolescents and young adults, not to mention situations such as the ingestion of drugs and other substances to escape the threat of these assaults of shame. Indeed, and as clearly mentioned by Yusuf et al. (2021, p. 240), youths who were attacked online "reported eating disorders, alcohol, drugs and substance abuse".

Several studies (Bauman & Baldasare, 2015; Li et al., 2020; Lee & Shin, 2017), resulting from theoretical reflections or field surveys, have tried to understand the prevalence, the etiology, the characteristics as well as the numerous consequences of this new form of crime or violence on young victims, but these remain still limited in the face of the constantly growing scale of the phenomenon. Although we did not perform a systematic literature review, that was beyond the scope of our study, we know from similar research (Chen et al., 2016; Even, 2019; Li et al., 2020; Marin-Cortés et al., 2019; Menesini et al., 2012) that most of studies on cyberaggression have focused more on children and in particular schoolchildren and adolescents, especially in developed countries, where the frequency of use of the Internet is particularly high (Petrosyan, 2022). However, these studies have paid less attention to what happens among young adults, especially among those who attend higher education institutions or universities; one of exceptions might be the study by Bauman and Baldasare (2015). As everyone knows well, these students are very keen on the Internet, video games and social networks, in particular because of (i) their level of education, (ii) their easier access to new information and communication and (iii) their relative autonomy. Furthermore, although they highlight various factors as being at the origin of these behaviors, studies on cyberaggression have not focused much on the role of the digital profile of young people (more or less use of Internet and social media sites for example) in the online aggression (Yusuf et al., 2021).

This study, based on an exploratory survey performed on a sample of Congolese students, has attempted to fill some of these gaps. The objectives of the study were threefold. First, it tries to determine the extent of the phenomenon of online aggression among university students before indicating how the prevalence of this phenomenon varies according to a certain number of socio-demographic variables. Second, it tries to identify the factors influencing participation as a victim or perpetrator of these online attacks before examining the respective impact of the hyperconnectivity of young people themselves. It provides some recommendations that can help reduce this phenomenon among college students in the Democratic Republic of the Congo (DRC). The study is be based on a conceptual framework presented in the next section and developed from our previous knowledge about aggression online and its effects (Chen et al., 2016; Even, 2019; Li et al., 2020; Marin-Cortés et al., 2019; Menesini et al., 2012).

3. CONCEPTUAL FRAMEWORK

Following are a couple of ideas around our study; they will be our logical line of reasoning in this investigation. First, studies on online attacks distinguish the victims from the perpetrators of these criminal acts, thus making it possible to highlight the profile of the aggressors and that of the victims. Our study combines the two groups and talks instead about young people involved in cyberaggression as victims and/or aggressors (or better perpetrators) with the aim of assessing the real extent of this phenomenon in our society. Second, to designate these acts of aggression on and via the Internet, several synonymous concepts are used in studies and research on the phenomenon. Thus, we sometimes speak of online aggression (cyberaggression), online violence (or cyberviolence), cyber-harassment, and especially cyberbullying, to distinguish them from traditional forms of violence between young people (Menesini et al., 2012; Yusuf et al. 2021). For our part, we prefer the concept of online aggression or cyberaggression, which seems to encompass various acts falling within this register, whether insults, dissemination of rumors, humiliating images, acts of harassment or identity theft on and via the Internet.

In this sense, despite the abundance of definitions encountered in the literature, we retain the following definition of online aggression: "an aggressive, intentional act perpetrated by an individual or a group of individuals by means of electronic forms of communication in a whether or not repeated against a victim who cannot easily defend himself" (Smith et al., 2008, p. 376). Such a definition highlights three important aspects of the phenomenon: (i) the existence of humiliating and nauseating acts on the net (Internet, social networks and other digital platforms) and recognized as such, (ii) the presence of a perpetrator (or group of perpetrators) and a victim, (iii) the intention to harm others, although this aspect is difficult to operationalize in studies. However, the repetitive nature will not be retained in this study, in the face of all forms of aggression, occasional or repeated.

To understand the development of these aggressive acts in cyberspace and grasp the main determinants among young Internet users, there are various analytical perspectives put forward in the scientific community. The first perspective considers that aggression online or on the Internet characterizes the new way of experiencing conflict between young people, given that they spend more and more time in the digital world and have the majority of their friends and acquaintances there (Mendez-Baldwin et al., 2015; Vale et al., 2018). All the conflicts and problems they encounter in the real world are mainly resolved in cyberspace. It is in this context that Vale et al. (2018) as well as Macilotti (2019) mentioned that "cyberaggression is the new form of interpersonal violence among adolescents". It appears that online attacks against young people are often "the result of arguments, teasing and face-to-face actions which are then continued on the internet". According to Macilotti (2019), these attacks are characterized by "a continuity between online and offline experiences".

One could also mention the idea that online aggression characterizes a certain specific category/profile of young people, although the phenomenon does not spare anyone. As such, young people with a certain profile are more likely to commit or suffer attacks online (Lee & Shin, 2017; Merril & Hanson, 2016; Mishna et al., 2010; Alvarez-Garcia et al., 2017). This perspective, which could be described as social determinants Another perspective, no less attractive, tends to underline that the increasingly frequent online attacks reflect the hyperconnectivity of young people (Athanasiades et al., 2016; Çakir et al., 2016; Cho et al., 2019; Gozlan, 2018; Park et al., 2014; Peker, 2015; Stahel & Weingartner, 2019; You & Ah Lim, 2016). According to the proponents of this thesis, cyberspace is now considered an extension of oneself. Social networks have changed communications, relationships and the very notion of intimacy (Gozlan, 2018). Authors like Tisseron (2003) even argues that these young people have "a desire for extimacy", which he defines by a "desire to communicate about his inner world to be validated in his existence, in his originality. This hyperconnectivity thus pushes young people to vent their anger and resentment there, as they would do offline, in the real world". There are other representations of cyberaggression among young people, ideas that deviate from these two mainstreams.

(Li et al., 2020; Stahel & Weingartner, 2019), underlines the existence of a certain number of factors at the origin of these attacks and which are more or less present among the perpetrators and/or victims of this phenomenon. This is the perspective we adopt in this study, the one that consists of examining the determinants of online aggression among young people.

In this very context, several studies (Alvarez-Garcia et al., 2015; Cho et al., 2019; Mendez-Baldwin et al., 2015; Vale et al., 2018) conducted among children and adolescents have shown that those who use more social networks and other digital platforms are more likely to experience online violence, but also to commit it. Vale et al. (2018), for example, showed that "a higher frequency of information and communication technology and cyber-practices/risks were associated with victim-perpetrators". Other studies have not found a strong link between the frequency of Internet connection and online aggression, but researchers are not ready to abandon this hypothesis, given the ambivalence of the results of the available studies. The question, which is also at the heart of our study, is therefore whether the probability of being the victim/perpetrator of an online attack depends on the digital profile of those concerned.

Another aspect refers to the parental control or intrafamilial communication. The role of parental control on children's digital practices has been pointed out in many studies (Mendez-Baldwin et al., 2015; Palermiti et al., 2017; Wright 2017; Vale et al., 2018; Zang et al., 2021; Larrañaga et al., 2016; Beyazit et al., 2017) considering, among others, that the existence of such control or of inter-family communication around this phenomenon reduces the risk of perpetrating or suffering aggression online. Although this awareness, little is known about the mechanisms (of this factor 's effect. Some studies also point to the role of parental control on children's digital practices and consider that the existence of such control or of inter-family communication around this phenomenon reduces the risk of committing or suffering aggression online, but mechanisms of the effect of this factor are not yet clearly elucidated. Although cyberaggression can affect all ages and populations, it has been reported in some countries and regions around the world that girls are more affected by the phenomenon than their male counterparts (Li et al., 2020). These studies do not make it possible to decide on this gender inequality in terms of online aggression, in particular because of the lack of control of other variables such as age, social background and family control.

Other authors mention, not without surprise, the overexposure of racial and ethnic minorities to violence on the Internet, particularly in terms of intimidation, but once again, this is not yet sufficiently supported by data from the field (Bauman & Baldasare, 2015; Merril & Hanson, 2016). While demographic factors such as age and sex, digital profile and parental control are cited as determinants of online aggression, other authors (Chang et al., 2015; Sasson & Mesh, 2017) also mention the risky behavior of some young people which overexposes them to this type of aggression or attacks. Among these behaviors we usually point out the exposure of young people to video games with violent content, the meeting with unknown virtual friends, the sharing of the connection with third parties, the publication of personal information. The younger people engage in these acts, the more likely they may commit and/or suffer attacks online. However, it is also necessary to take into account the personality traits of these young people which could contribute to the reinforcement or, on the contrary, to the reduction of the risks incurred (Antipina et al., 2020; Brewer & Kerslake, 2015; Festl & Quandt, 2016; Malinowska-Cies'lik et al., 2022). In this regard, no one is unaware of the impact that men's psychological attributes (openness, conscientiousness, extroversion, friendliness and narcissism to consider the big five personality traits, as defined by McCrae & Costa (1987), exert on the human actions and behaviors. Instead of these key traits of personality, some authors (Brewer & Kerslake, 2015; Palermiti et al., 2017; You & Ah Lim, 2016; Yusuf et al., 2021) point out the role of self-esteem as key psychological determinant of online aggression.

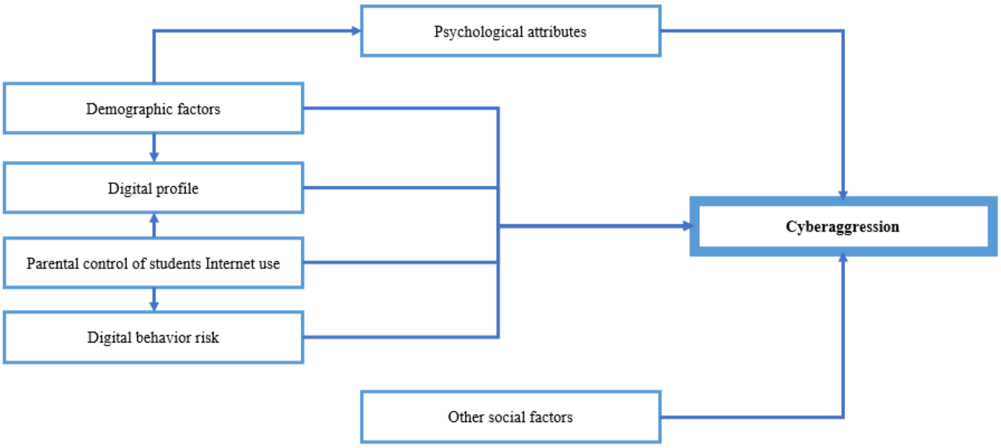

Figure 1. Our proposed conceptual scheme for the study of cyberaggression factor risks
Source: developed by the authors

As we can notice it, online aggressions (or cyberaggression) can be the result of different factors of various kinds, and the most important of them would be, according to some literature, the digital profile, the degree of parental control of students Internet use, some demographic factors, digital behavior risk, personality type and other social factors, as we have schematized in the above diagram (Figure 1). To what extent do these factors influence online aggression among Congolese students? This is one of the two research questions addressed in this study and outlined above. After these theoretical considerations, we are going to describe how we have tried to gather relevant data and analyze them to try to answer our research questions.

4. GENERAL INFORMATION ON CYBERAGGRESSION

After defining the context of this study and setting out the methodological approach adopted in the exploitation of the results of the survey carried out, we take advantage of this section to open a brief parenthesis in order to recall some basic concepts relating to cyber aggression. For a better understanding, we organize the rest into three subsections: the first deals with the place of the Internet in our lives, the second discusses the relationship between young people and screens, and the third presents the dark side of the Internet in relation to online aggression. The third analyses the dark side of the Internet by considering it as a dangerous world.

4.1 A Connected World

In this modern world, in the major cities of developed and developing countries, it is almost impossible to find a home where the Internet is not present. Thanks to the Internet, our contemporaries have become dependent on numerous applications and/or software that are indispensable for chatting, entertaining, checking accounts, organizing a trip, ordering shopping and even DIY at home. When it comes to IT and digital equipment, we are seeing technological advances in the power and capacity of smartphones, tablets, and computers. Despite everything, of all the regions in the world, the African continent remains the least concerned by new information and communication technologies, even though 40% of its population is connected to the Internet. In fact, the International Telecommunications Union (ITU) reveals in its report on connectivity in 2022 that the continent is not out of the woods as far as the digital divide is concerned, but there has been steady growth in Internet penetration in recent years. Regardless of the country, all young people live in an increasingly dematerialized world where they access and are confronted with multiple digital objects via the Internet. These gadgets have found the means to validate the new revolution that is taking place with the ever-increasing presence of connected objects in our lives and in almost every sphere of activity. These objects include everything from the most trivial to the most useful: thermostats, thermometers, bathroom scales, watches, lighting, earphones, shower heads, voice assistants, forks, cooking robots, dolls, pollutant detectors, etc.

It is a fact that young people rarely look for information; it comes directly to them, usually via software installed on smartphones, tablets and/or computers. What's more, new forms of human-machine-human interactivity are being introduced (tactile, vocal, olfactory, etc.) to interact with these sometimes highly sophisticated connected objects. In this sense, the Internet of Things (IoT) is accelerating technological change by changing the way we interact with everyday objects. In other words, the sensors in these connected objects are set to transform not only our lives, but also factories, warehouses, logistics and, more generally, the entire industrial value chain. The enormous quantity of data produced is at the heart of big data, when conventional methods of storage and processing are no longer sufficient. With home automation, the automation services built into doors, windows and household appliances offer real comfort in our homes. For example, it's possible to regulate and start the heating in your home remotely from your tablet or smartphone. Similarly, we can rely on smart cameras to ensure the security of our homes and/or offices. These devices now have functions that enable them to differentiate between the presence of animals or humans. And in the event of an intrusion, these cameras send an alert message directly to the owner's smartphone. Furthermore, the concept of the "smart city" has been part of our vocabulary for several years now. The political and/or administrative leaders of major conurbations are working with experts to redefine new ways of getting around, heating, eating, treating rubbish and organizing community services, considering the powerful functionalities of connected objects. They introduce a new dimension to ecology, integrating the impact of digital transformation on the fabric of cities and regions. In this sense, the notions of "smart city" and "sustainable city" remain closely linked, as digitalization is not in itself definitive, but simply a new technical and IT opportunity to serve a sustainable city.

It should also be pointed out that the digital transition is having such a technological, organizational, and cultural impact on society that it is also raising new political issues that absolutely must be taken into consideration. Indeed, with the major concern of limiting atmospheric pollution as much as possible, digital technologies are setting the pace for the construction and operation of modern cities. In this sense, it would not be an exaggeration to regard this concern as a strategic issue, given that urban consumption accounts for almost half of household spending in most developed and developing countries. However, the management of this consumption suffers from several dysfunctions including, but not limited to, housing price policies, air pollution and/or transport congestion. Unfortunately, the offers put forward by the digital giants under the concept of the smart city are leading to far-reaching changes in the way cities function, whether in social, urban planning, ecological or political terms. In industry, the 4.0 revolution is revisiting all processes, from production to logistics. In this respect, the IBM teams state that "we are witnessing the materialization of the digital transformation of industrial operations in all areas, with real-time decision-making and increased productivity, flexibility and agility". The 4.0 revolution is also completely changing the logic of the design, manufacturing, and distribution processes for industrial products, with the integration of new information and communication technologies (NICTs) such as cloud computing, the Internet of Things (IoT), data analytics and artificial intelligence.

While emphasizing the comfort we enjoy thanks to the digitization of our personal activities, our homes, our cities and our industries, the interest of this book is to echo the other side of the coin of these new technologies by mentioning the dangers that accompany these tools including:

- destabilization: disruption of operations, damage to image or sabotage;
- espionage: theft of technology and know-how and;
- cybercrime: ransomware, fraud, data theft and blackmail.

4.2 Young People and Screens

Far from weighing up the pros and cons of screens in our lives, the idea behind this section is simple: to highlight their presence in our living environment. Smartphone, tablet, television, computer, or video games console: screens are part of everyday life in most families, and children generally love them. Screens are now part of our daily lives, and perhaps even more so in these post-confinement times when teleworking and e-learning are becoming the norm. From young children to the elderly, when it comes to questioning the consequences of more or less intense screen use, from parental advice to spotting real addictions, GPs seem to play a key role in preventing excessive exposure to screens, especially for the very young. In all cases, the ideal would-be moderate use of screens in order to reduce the associated risks while reaping the benefits.

Above all, we all have one of the most important connected objects, one that can be described as universal in two ways: firstly, it's everywhere, and its penetration rate is extremely high. And secondly, because it works through applications, it can be used for everything. Clearly, smartphones are magical when they are equipped with multiple sensors that can be used to build all kinds of applications, such as photo, video, microphone, proximity, luminosity, magnetometer, gyrometer, fingerprint, voltmeter, thermometer, or hygrometer. What's more, smartphones are almost constantly connected, particularly for young people.

Our eyes are on a smartphone, our fingers are on a tablet or a computer keyboard... Screens play a very important role in our lives! Thanks to Snapchat or Instagram, we can always chat with friends, spend hours watching videos on YouTube, choreograph on TikTok or play Fortnite with people on the other side of the world. Basically, the advent of smartphones and other tablets that are now part of our daily lives has given a huge boost to the creativity of manufacturers and opened up a field of new and very interesting applications: the intelligent home (which controls the opening of doors, regulates the temperature, turns the lights on and off, etc.), a car that warns when it needs to be refueled, an electronic bracelet to monitor health and warn people when parameters change, etc. Critics of the mobile phone claim that it causes attention and sleep disorders in young people, prevents them from concentrating effectively on lessons, dangerously reduces their physical activity to almost zero, exposes them to shocking images, whether pornographic or simply violent, destabilizes them greatly and, above all, exposes them to cyber-attacks. This last aspect is the leitmotif of this document and the subject of the following lines.

4.3 A Dangerous (Virtual) World

From the foregoing, the world, and young people, cannot do without the Internet. In fact, these days, young people easily acquire the necessary technical skills related to the online world. As a result, they quickly learn to surf the Internet with smartphones, tablets or computers and, above all, to spend time on social networks. For parents, the task can be a little more difficult. In fact, sometimes it's just when teenagers feel comfortable on a social network. Often, they start just as young people are moving on to other things. The example of Facebook in the face of the rise of Instagram, Snapchat and, more recently, Tiktok is a perfect illustration of this. However, while young people enjoy a certain amount of technological freedom, they lack the psychosocial skills to recognize the possible consequences of their actions. This is perfectly normal and can be explained by their young age and the fact that certain parts of their brain are not yet fully developed. So, we need to support them and make them aware of the dangers of the Internet. In other words, the advent of information and communication technologies (ICT) has created new opportunities to harm others, with potentially more serious consequences for the victims. In other words, with the growth of cyberspace, and in particular the proliferation of connected objects, malicious activities are becoming both more numerous and more sophisticated. Generally speaking, deviant behavior is found all over the world, committed online, particularly on social networks or via mobile communication systems, for instance: SMS, MMS, video, etc. and classified as intentionally harmful to a person or group of people, whatever their age, who find these acts offensive, derogatory, harmful or undesirable. ICTs have rapidly become a ubiquitous part of everyday life, allowing people to engage in aggressive behavior on many different platforms with different capabilities. Modern internet media allow users to upload objectionable text, edited and unedited images, audio and video files. However, it is not just the content of the message that makes a cyber-attack unique. ICT features facilitate anonymity, planning, perseverance and reflection. What's more, the visual, emotional, and physical distance between perpetrators can make cyberattacks feel more at ease. Finally, online contexts allow people to choose their target audience, viewers and victims, maximizing the extent of the damage they cause and minimizing the consequences. These behaviors are referred to in the literature as cyberaggression or cyberattack.

Generally, a cyber-attack is defined as any act of attack against a computer device on a computer network. A cyber-attack may come from individuals or a group of hackers, possibly belonging to the government. A cyber-attack is almost always harmful but may be ethical if its sole purpose is to draw attention to a security flaw. A cyber-attack, on the other hand, targets an individual or a group of people who share a common characteristic. Young people often engage in online aggression without even realizing it. In this sense, cyber aggression is defined as any behavior committed with the intention of harming someone using a computer, mobile phone or other electronic device. For example, having a negative conversation about another person online. Cyberbullying can also be as simple as liking a negative comment on someone's social media feed that the author may not know is negative. Cyberbullying in the workplace takes the form of threatening or intimidating emails or text messages. It can also include emails or text messages with objectionable content, such as sexist or racist material, or expressions of religious hatred or homophobia. What distinguishes this form of aggression from more traditional forms is that it is not limited to colleagues but can come from outside the organization and can also take the form of spam.

The phenomenon of cyber-aggression seems to have its roots in young people who have grown up with the Internet and electronic communications (Runions et al., 2018). They have brought this intimacy into the workplace and are unaware that this cyber-attack in the workplace is just as damaging as any other form of attack. In the workplace, cyber-attacks are often carried out by people who are offended, angry or threatened with anger, and who resort to this form of virtual communication in retaliation. According to the InfoSci (IGI Global, n.d.) dictionary, cyberbullying is an aggression between peers that occurs once or occasionally online. As well as being temporary, the dictionary points out that in a cyber-attack there is no imbalance of power between the attacker and the target and that there is generally no intention to cause harm or injury. In other words, it is a relational phenomenon in which one person in an online environment intimidates, emotionally hurts or exercises power over another. Unlike cyber-attacks, cyber-bullying is a repetitive aggressive behavior designed to cause great harm while creating an imbalance of power between the source and the target. It is characterized by the fact that it is carried out through online contact. The electronic medium highlights other potentially relevant elements such as greater anonymity and the 24/7 nature of the Internet. We also define cyberbullying as a form of harassment committed through a series of hostile acts, the repetition of which mentally weakens the "victim". Any aggressive behavior committed repeatedly and intentionally by a person or group of people is harassment. This behavior is always directed against another person or group of people. Cyberbullying can take one of six forms:

1. Identity theft

Identity theft is the crime of stealing another person's personal information and using it for fraudulent purposes, usually for financial or romantic purposes online. In the event of identity theft, the following information may be stolen: name, address, telephone number, social security number, login details (username/password), bank statements and/or account numbers and details, credit card number or biometric data. Identity theft, literally, can involve looking for personal information in discarded documents or rubbish bins, or stealing it directly from an individual. It can also be cybercrime, where malicious actors steal information or data through fraud, malware, hacking or security breaches. Identity theft is generally impersonation, i.e., the use of another person's personal information without their consent. Identity theft is when someone pretends to be someone else. Identity theft involves stealing information, gaining access to confidential resources or obtaining financial gain. Financial losses caused by identity theft continue to rise:

2. Doxing

Sometimes spelt doxxing, is the disclosure of information that identifies an individual online, such as name, home address, place of business, telephone number, financial information and/or other personal information. This information is then disclosed publicly without first seeking the victim's consent. Although the disclosure of personal data without an individual's consent predates the Internet, the term "doxing" first appeared in the 1990s in the world of Internet hackers, where anonymity was sacred. Feuds between rival hackers sometimes led to someone deciding to "manage" someone else previously known only by a username or nickname. "Documents" became "dox" and finally a verb in its own right (i.e., without the prefix "drop"). As a result, the definition of doxing has expanded beyond the hacker community to include the disclosure of personal information. While the term is still used to describe the unmasking of anonymous users, it has lost its meaning today as most of us use our real names on social networks. More recently, doxing has become a tool in the culture wars, where rival hackers intimidate opponents. The goal of doxers is to escalate the conflict with their targets from the online world to the real world by disclosing information such as: home address, work information, personal phone numbers, national insurance numbers, bank or credit card account information, private correspondence, criminal records, personal photos, embarrassing personal information. Doxing attacks can be relatively harmless, such as fraudulent e-mail registrations or pizza deliveries, or far more dangerous, such as harassment of a person's family or employer, identity theft, threats or other forms of cyberbullying, or even personal harassment. Drunk people include celebrities, politicians and journalists who endure online mobs fearing for their safety and, in extreme cases, receiving death threats. The practice has also spread to senior business leaders; for example, when Gillette, a subsidiary of Procter & Gamble, released a 'We Believe' advert to combat toxic masculinity, brand leader Marc Pritchard's LinkedIn profile was shared on 4chan, along with a poster urging others to speak ill of him, complete with hate messages. Doxing can be triggered by a feeling of having been insulted or attacked and, in turn, taking revenge for the harm done. People may also react and attack in order to express a contradictory opinion. Perpetrators sometimes see their actions as a means of redressing perceived wrongs. Whatever the cause, the decision to intentionally disclose personal data online is generally intended to intimidate, punish or humiliate the victim.

3. Swatting

Swatting involves a perpetrator contacting law enforcement and making a false report about someone. A SWAT team (Special Weapons Attack Team) may then burst into the victim's home. The aim is often to get the police to storm the house while the target is online, perhaps streaming live audio or video. The perpetrators often take their actions as a joke, but they can have serious consequences. The incident keeps police response teams on their toes and prevents them from responding to real emergencies. There have even been accidents in which police officers have been killed, and in one case the victim was killed by police officers. The United States is steadily increasing penalties to deter the perpetrators of these jokes, but the problem remains unresolved, as many of the perpetrators use sophisticated techniques to operate anonymously by impersonating others or using internet telephony software.

4. Trolls

If you have been using the Internet for a long time, there is a good chance that you have come across a troll. An Internet troll is someone who intentionally makes derisive, rude or disturbing statements on the Internet in order to evoke strong emotional reactions in people or divert the conversation away from the subject at hand. They can take many forms. Most trolls do it for fun, but other forms of trolling have a purpose. Trolls have been part of popular and fantasy literature for ages, but online trolls have been around for as long as the Internet has existed. The first known use of the term dates to the 1990s in the first online discussion forums. Back then, it was a way for users to mislead new members by repeatedly posting an insider joke. Since then, it has evolved into much more harmful activities. Trolling is different from other forms of cyberbullying or harassment. It is not usually aimed at one person but is designed to attract attention and provoke others. Trolling occurs on many online platforms, from small private chat groups to large social networks. Here's a list of places on the internet where you're likely to see internet trolls:

- Anonymous Internet forums: places like Reddit, 4chan and other anonymous discussion forums are popular places for Internet trolls. Because there is no way to trace a person's identity, trolls can post highly provocative content without repercussions. This is especially true when forum moderation is lax or inactive.

- Twitter: which also offers the option of anonymity, has become a mecca for trolls on the Internet. Common trolling methods on Twitter include hijacking popular hashtags and mentioning popular Twitter personalities to get the attention of followers.
- Comment sections: comment sections on sites such as YouTube and news sites are also troll favorites. There are several obvious trolls who often provoke numerous reactions from angry readers or viewers.
- Trolls are everywhere online, including Facebook and dating sites. Unfortunately, they are quite common.

5. Revenge porn

Revenge porn refers to a situation where a person publicly discloses sexual photos or videos of an ex-partner without their consent. It refers to a situation where a person publicly discloses sexual photos or videos of an ex-partner without their consent. The term revenge originally referred to the practice of getting back at an ex-partner by intimidating them or forcing them back into a relationship. The term has now been broadened to include the distribution of any sexual content by anyone (ex-partner or not) without their consent (even if the recording was originally made with their consent) for any reason whatsoever. This sexual content can also take the form of text messages, videos, photos, etc. Revenge porn is not the official name for this crime, but it is a commonly used and understood term. It is a sexual offence that usually, but not always, involves a member of a couple or ex-couple publishing intimate photos of their partner, usually an ex-partner, without their consent. This is known as revenge pornography because the act is often a form of revenge for something the other partner did wrong or wanted to do. Reported cases of revenge pornography have increased considerably in recent years, as mobile phones are more powerful and most of them are equipped with cameras. So sharing photos has never been easier. Sharing photos has never been easier. For this reason, more and more people are sharing intimate photos with their partners via social networks, text messaging and other instant messaging services. Originally, a person could trust their partner enough to share such personal information with them and ensure that the recipient was not acting maliciously enough to share it with others. If these private images become public without the partner's consent, or threaten to do so, this is called revenge porn. Once an image is shared online, the author loses control of where it is and the image can be downloaded again and shared by a large number of people. So sharing someone's image on the Internet can have devastating effects on people's lives and work, causing problems not just immediately, but for months and years to come. With people spending more and more time on the phone, the temptation to send a photo to get back at an ex has never been greater. What may seem like a short-term victory when you share someone's photo can actually lead to serious complications and jail time. Revenge porn" is a form of harassment that can have serious consequences for the victim. First of all, the emotional consequences. The images or texts in question can in fact provoke harassment from those who have seen the material in the media or damage the victims' reputation. The latter may also suffer professional consequences. Of course, the consequences can be even more serious when the victims are minors. We therefore urgently needed to find a solution in Belgium to enable us to continue these activities and stop transmitting the images as quickly as possible.

6. Cyber stalking

Cyberstalking is a form of cybercrime that uses the Internet and technology to harass or stalk someone. It can be seen as an extension of cyberbullying and personal harassment. However, it takes the form of text messages, e-mails, posts on social networks and other media, and is often persistent, deliberate and methodical. Cyberbullying often begins with seemingly innocuous interactions that then become routine in annoying or frightening ways. Some even find the early stages of cyberbullying fun and harmless, but it ceases to be fun once the interactions continue, even after the recipient has expressed disappointment and asked for the interaction to end. Content aimed at victims is often inappropriate and disturbing. A cyberstalker may frighten his victim by sending messages several times a day and from different accounts. Cyberbullying does not necessarily require face-to-face communication, and some victims may not even realize they are being harassed online. Victims can be tracked in a variety of ways, and the information gathered can then be used to commit crimes such as identity theft. Some stalkers even go so far as to stalk their victims offline and contact friends. Typical features of cyberbullying include harassment, invasion of privacy, online and physical surveillance, compulsive tracking of victims' location, intimidation of victims, etc. Stalking on social networks can include threatening private messages or fake photos. Cyber-stalkers often make false accusations, spread malicious rumors, create fake profiles or blogs on social networks, or create and publish revenge pornography. You may mistakenly believe that cyberbullying isn't as serious as physical harassment because it doesn't involve physical contact. The Internet has become an integral part of everything we do, both personally and professionally. This has only facilitated communication and access to personal data. On the other hand, cyberbullying is essentially the sending of electronic messages that intimidate or threaten the recipient, while cyberbullying refers to the repeated use of electronic communications to harass or intimidate another person. Being a victim of cyberbullying or cyberstalking can have a negative impact on a person's physical and mental health, academic performance, confidence and relationships, in addition to causing physical or psychological harassment.

4.4 A World to be Lived Carefully

As described above, the infiltration of information technologies into every segment of the world's population and the digitization of almost all our daily activities are also accompanied by hostile and indecent behavior, such as insults, threats, possible sexual harassment, disclosure of personal data, sharing of sexual relations without consent and cyberbullying. Unfortunately, all too often, the online world is still not seen as "real life", but we need to make young people (and the not-so-young) aware that everything that happens online can have very real consequences. In the case of cyberbullying, for example, virtual violence inflicts very real harm on the victim. Please note that content posted as a threat or insult can result in criminal prosecution. And these days, even the simple act of liking or sharing can lead to more and more justice. So, there is a risk of criminal prosecution, and it's important to remember that not everything is legal on the Internet.

The preceding few lines sufficiently demonstrate the place occupied by the Internet in our lives, particularly those of the younger generations over the last ten years or so. They use these tools to communicate, reproduce, create and share content, following the logic of media. In this context, digitization contributes to the development of a "participatory culture" on the Internet (Jenkins, 2006), and the virtual environment becomes a place of openness to others, a space for socialization and the reinforcement of social capital. The Internet also has many positive aspects and can be used to promote learning and empower young people. While highlighting the opportunities that the Internet offers young people, we've taken the opportunity of this section to emphasize the risks to which they expose themselves by navigating this virtual world. So, to protect those at risk of online addiction, bullying and aggression, more research is needed to identify them and develop targeted measures to keep them out of harm's way. This article contributes to this noble goal by presenting the results of a survey of young Congolese students.

5. PARTICIPANTS AND METHODS

5.1 Participants

Data used in this study have been collected from a sample of 1,500 participants who are currently university students from two Congolese universities (Catholic University of Congo, CUC, https://ucc.ac.cd/ and New Horizons University, NHU, https://www.unhorizons.org/) located respectively in Kinshasa and Lubumbashi, the two biggest cities of the DRC; more information around the survey can be found in Mbaki Luzayisu & Zamwangana Tungu (2023). As shown in the Table 1, there is a balanced number of female and male participants. Participants ages range between 18 and 30, with a higher share of those aged less than 20 years old. Students aged more than 24 years made up 14% of the total sample. Furthermore, participants mostly live with their (biological or non-biological) parents and are from large families (families with 5 children and more). Of the students surveyed, the majority (75%) is studying first grade of university, 10% are in second grade, 15% in higher grades (Table 1).

All the participants have been selected at random among those who have been enrolled in both Universities and have followed any computer science course since 2020 with one of the two paper's authors; he keeps a long list of email addresses made up of more than 8,000 students. The field work took place in November 2022.

Table 1. Breakdown of study participants by various socio-demographic attributes

Variable	Category	Frequency	Percentage*
Age group	18-20	705	48%
	20-22	400	27%
	22-24	170	11%
	24+	207	14%
Sex	Female	747	50%
	Male	748	50%
Family residence	Live with biological parents	1086	72%
	Live with other parents	131	9%
	Live with friends & acquaintances	26	2%
	Live with other persons	258	17%
Nb of siblings	1	57	4%
	2	88	6%
	3	184	12%
	4	229	15%
	5	287	19%
	6+	652	44%
Elder position or not	Elder	472	32%
	Other position	1025	68%
University grade	First grade	1128	75%
	Second grade	154	10%
	Third grade	91	6%
	Higher grades	128	9%

* Percentages calculated from the total number of participants (1500) with valid answers.
Source: developed by the authors using survey data.

5.2 Questionnaire

An ad hoc questionnaire with sixty five questions/items has been prepared and submitted online to all the participants who filled in it without any human assistance (self-administered questionnaire). This questionnaire contains ten questions concerning students' attributes (date of birth, gender, number of siblings, mother language, school grade, family residence to name only a few) and use of electronic devices, Internet and social media sites as well as the usage frequency and duration of Internet. The questionnaire also contains students experience about posting/publishing contents on the Internet and friendship management online to assess their online behavior risk in terms of online aggressions. One questionnaire's module has been devoted to cyberaggression measurement using a set of items likely to occur online. Along with items regarding parental control and student knowledge and attitudes towards online aggression, a few questions have been also used to evaluate student self-esteem and their sociability level.

5.3 Data Analysis

Gathered data were analyzed using the SAS software package, especially its SAS/STAT module (version 15.2). Firstly, all the distribution of participants by study questions/items have been examined to ensure data quality and gather preliminary insights. That also allowed (i) to evaluate composite indicators such as online behavior risk, propensity to be victim and/or author of online aggression and connectivity level; (ii) and to better understand students' digital usage patterns. Secondly, the prevalence of cyberaggression was analyzed in terms of frequency and percentages as well as associations between cyberaggression and various participants attributes. Finally, the factors associated with the cyberaggression were identified using logistic regression analysis.

We used logistic regression technique to examine the effect of different explanatory variables on the probability of being a victim and/or perpetrator of online aggression. This last variable is based on two values: if the student has already been a victim and/or perpetrator, the variable takes the value 1, otherwise 0. The binary nature of the variable makes it favorable to logistic modelling. We had six groups of explanatory variables: demographic factors (age group, sex, siblings, promotion and rank in the family, used separately in the model), digital profile (low user, medium and heavy Internet user), the digital risk characterizing the students in 3 groups (low risk, medium risk and high risk), the psychological factors grouped around self-esteem and the conflicting nature or not of the student in his living space, parental control of students Internet use as well as other variables such as knowledge of articles and laws on cyberaggression as well as the attitudes to adopt at the University in the face of an online attack. Results of logistic regression are interpreted in terms of odds ratios, obtained by the exponentials of regression coefficients (exp. (ß)), along with their associated p-values to evaluate their statistical significance. Only direct effects of different factors are considered. Hence, the main focus was to present the effect of each retained factors on cyberaggression; no interaction effects have been included in the final model, because the level of interrelationships (or associations) between risk factors was low. Data also showed that following logistic regression assumptions were met (independence of observations and no perfect multicollinearity of risk factors). To cope with the lack of linearity, each of the categorical variables has been transformed into buckets and then into dummy variables that were included in the model. Main results obtained using logistic regression are presented in the next section.

6. RESULTS

6.1 Digital Usage Patterns among Participants

Before reporting our main findings on the prevalence of and factors affecting online aggression s, we first give some digital usage patterns characterizing participants (Table 2). The results show that most of the participants (94%) use smartphones to navigate on the Internet and only a few of them still go to cybercafés for that (Table 2). Participants also use the Internet almost daily (93% use it at least 5 days per week) for things other than university work. They reported also have used social media sites in the previous 12 months before the survey: WhatsApp is the most used application with 99% reporting this usage and Twitter being the least used one. The majority of the participants (63%) reported spending more than 2 hours online and at least 10 dollars per week when they go on Internet. Most of them (77% in total) reported that they regularly publish various contents (photos, images, videos and personal info) on the net (Table 2). An important share of participants do share the internet connection with other when they are running out of credit. Our surveyed students also reported that they mainly use WhatsApp to communicate with their parents: the channels such as text messages (SMS), phone calls and emails are less and less used in the student's ecosystem. We'll talk about the prevalence of cyberaggression among study participants in the next section.

Table 2. Key digital usage patterns among study participants

% of students accessing the web via their smartphones	99%
% of students who access the web via cybercafés	19%
% of students reported have used the following social media sites in the previous 12 months	
- WhatsApp	99%
- Facebook	78%
- Tiktok	73%
- Instagram	76%
- Snapshot	78%
- Twitter	38%
% of students communicating with parents via WhatsApp	90%
% of students spending at least 2 hours online per day	53%
% of students using the web between 5 and 7 days per week	93%
% of students spending at least 10$ per week for the internet	68%
% of students who have published contents on the internet in the previous 12 months	77%
% of students who have used Excel or Word applications in the previous 12 months	70%

Source: developed by the authors using the survey data.

6.2 Prevalence of Cyberaggression among Participants

Based on the combination of all items related to cyberaggression submitted to the participants to evaluate and characterize the rate of participants being victim or authors of cyberaggression during the previous 12 months preceding the survey, the following results have been gathered:

- 61% of participants did not report any experience of cyberaggression during the reference period;
- 32% of participants have reported at least one of the aggression experiences as victim only;
- 5% of participants have reported any experience of the aggregation experiences as both victim and author during the period of reference;
- 2% of participants have reported any experience of cyberaggression as perpetrator only.

Putting all together, the overall prevalence of cyberaggressions has been estimated to 39% of participants having involved in cyberaggression as victims and/or author during the study period. This relatively high prevalence of cyberaggressions among surveyed students could be linked to different factors such as their high connectivity and high risky of their digital behavior, as suggested in our conceptual framework. The results concerning these relationships are developed in the following section of the paper.

6.3 Factors Associated with Cyberaggression among Participants

Table 3 provides information about the effect of the factors investigated in the analysis using logistic regression. Among others, the table highlights all the odds ratios (OR hereafter) and p-values associated with each of the variables. To evaluate if the effects are statistically significant, we have relied on the p-values less than 0.05. Such small p-values mean that there is a small probability that the effect observed is due to chance. In other words, it's the probability that the null hypothesis is true, as usual.

Considering digital behavioral risk, one of the facets of students' connectivity, we found the following 3 groups: (i) students with low digital risk (19%), (ii) those with moderate digital risk (58%) and (iii) those belonging to the high digital risk group (23%). As we can see, nearly 80% of the students surveyed are in fact in a situation of moderate or high risk of cyberaggression. Results showed a significant correlation (OR=1.51; p-value=0.0001) between high digital risk and probability of being victim or author of cyberaggression. Furthermore, as already mentioned, the majority of the participants (80%) have high or medium digital connectivity that results from their usage frequency and duration of Internet and social media sites use in the previous 12 months. There is a good correlation between digital connectivity and cyberaggression, but it's not statistically significant (OR for high digital connectivity is 1.14; p-value=0.1488 and OR for medium connectivity is 1.05; p-value=0.5746). Results also showed that 43% of participants belong to families where parents or tutors discus with their children about the risk of online aggressions (Table 3). Significant correlation was found between parental control of internet usage and probability to be victim and/or author (OR =0.878; p-value=0.045). Speaking about parental control, it is also important to mention the effect of living together with biological or non-biological parents vs. other relatives or friends. Results revealed that participants who live in the former type of environments are significantly less likely to be victim and/or author of cyberaggression than their counterparts living without parents (Table 3).

Results also revealed the effects of psychological attributes used in the study (Table 3). There is a significant correlation between associability level and online aggression. Compared to those who are conflict averse, participants who tend to have hot discussion or arguments with their friends are more likely to be victim and/or author of cyberaggression (OR=1.873; p-value=0.001), but participants self-esteem measured through the Rosenberg scale (Rosenberg, 1965) and cyberaggression are not significantly linked. With regard to the demographic variables analyzed, gender obtained an unexpected result. According to prior available evidence, female exhibit higher cyberaggression than male students, but the data obtained in this study showed that every other things being equal there is no significant correlation between gender and the probability of being a victim and/or author of cyberaggression (OR=0.942; p-value=0.373). However, results revealed significant effect for age and university grade. Participants studying in first university grade do experience high probability of being victim and/or perpetrators than those enrolled in the highest grade (Table 3). Those key results will be discussed in the next section.

Table 3. Results of logistic regression of students' attributes on the propensity of being victim and/or author of online aggression

Variable	Parameter	Standard Error (SE)	Chi-Square (Wald stat.)	P-value	(Odds ratio)**
Intercept	-0.2588	0.316	0.6712	0.4126	
High internet user	0.127	0.088	2.08	0.1488	1.136
Medium internet user	0.049	0.089	0.31	0.5746	1.051
Low internet user (ref..)	****				1.000
High digital	0.4081	0.104	15.34	0.0001	1.504*
Moderate digital risk	0.0369	0.085	0.19	0.6636	1.038
Low digital risk (ref.)	****				1.000
Knows laws & instructions	0.051	0.073	0.486	0.486	1.052
Do not know laws & instr. (ref.)	****				1.000
Agree with academic sessions	-0.059	0.088	0.448	0.503	0.943
Do not agree (non) (ref.)	****				1.000
First grade	0.3904	0.163	5.737	0.017	1.478*
Second grade	0.1298	0.212	0.375	0.541	1.139
Third grade	-0.2366	0.252	0.882	0.348	0.789
Fourth grade	-0.2672	0.397	0.452	0.501	0.766
Fifth grade (ref.)	****				1.000
18-20 years old	-0.2376	0.3257	0.5323	0.4656	0.788
20-22 years old	0.4948	0.1801	7.5447	0.0060	1.640*
22-24 years old	-0.1253	0.1906	0.4318	0.5111	0.882
24+ (ref.)	****				1.000
Female	-0.0594	0.066	0.794	0.373	0.942
Male (ref.)	****				1.000
Parental control (oui)	-0.013	0.065	4.017	0.045	0.878*
No parental control of internet use	****				1.000

Elder among siblings	0.0801	0.071	1.284	0.257	1.083
Other position among siblings (ref.)	****				1.000
Nb of siblings	0.0133	0.026	0.286	0.611	1.013
Strong self-esteem	0.0639	0.0914	0.488	0.4848	1.066
Medium self-esteem	0.0848	0.0911	0.867	0.352	1.089
Low self-esteem (ref.)	****				
Argue much with friends	0.6276	0.1342	21.88	0.0001	1.873*
Argue a little with friends	-0.1320	0.0935	1.993	0.1580	0.876
Do not argue with friends (ref.)	****				1.000
Live with biological parents	-0.2861	0.1515	3.5654	0.059	0.751*
Live with other parents	-0.2817	0.2052	1.8844	0.170	0.754
Live with friends or acquaintances	0.5979	0.3664	2.6622	0.103	1.818
Live with other persons (ref.)	****				1.000
Have many friends	-0.1244	0.1226	1.029	0.3104	0.883
Have few friends	-0.1919	0.1245	2.377	0.1231	0.825
Do not have friends (ref.)	****				
Sample size Number of valid responses Pearson's Chi-Square Pr>ChSq	1500 1235 91.3 <0.0001				

*Regression coefficient is statistically significant at 5% ; ref = reference category.

Source: developed by the authors using survey data.

7. DISCUSSION, STUDY'S LIMITATIONS AND RECOMMENDATIONS

The aim of this study was to examine the prevalence and risk factors of online aggression among university students in Congo. Online aggression is becoming a serious problem among young people and adults who are avid of Internet and undertake risky behavior online that overexposing them to various attacks. Up to date, a lot of studies have been conducted to better evaluate and understand this social phenomenon. While most previous studies addressed the phenomenon among children and adolescents in Europe, America and Asia, our study has been undertaken among university students in Africa; those students intensively use Internet for both university work and entertainment such as sending and receiving text messages, publishing contents and other personal information on the web. Our study also put a specific focus on the students hyperconnectivity as the key driver of their involvement in cyberaggression context as suggested by many researchers. In the same vein, and contrary to many previous studies, we have built a clear conceptual framework which suggests that cyberaggression among students could be considered as an output of a combination of several and different factors including demographic factors, digital behavior risk, digital profile, parental control of student's internet use and psychological attributes that describe students personality. Finally, the study relies on an exploratory fieldwork; we developed an ad hoc questionnaire that we submitted to the participants who freely answered online without any human assistance, although they were not selected through a clear random sampling procedure.

First results do not necessarily confirm all the suggested hypotheses, while a few of them are consistent with the literature and our conceptual framework. Most of the previous researches emphasizes the gender differences, but we did not find any evidence of significant correlation between sex and online aggression. Hyperconnectivity that some researchers considered as key driver of online aggression find echo in our study. We found that students who undertake highly risky behavior online such as sharing the internet connection with others, publishing contents online or having dates with virtual friends, are among those who experience higher probability of being victim and/or perpetrator of online attacks. Parental control of students Internet use is also consistent with the literature, as students living within families where there is family communication around the internet have lower probability of being victim and/or author of online attacks; these finding echoes previous research in the parental involvement in the cyberbullying reductions (Larrañaga et al., 2016; Mendez-Baldwin et al., 2015; Beyazıt et al., 2017). Psychological based attributes such as student self-esteem seem not to be significantly associated with the aggression in the Internet, although the clear theoretical mechanisms suggested in the literature and some empirical researches (Brewer & Keslake, 2015; Palermiti et al., 2017). Beyond risk factors of cyberaggression, the results contribute to a better understanding of students' use of Internet and social media sites. They also raise the need for deeper researches on cyberaggression among students in DRC to better understand mechanisms underlying the effects of different risk factors identified in this study; they have not been addressed here.

Although those contributions, some limitations should be considered. First, this study was not based on a random sample; this fact limits the inference of our results to all Congolese students. Second, methodology used to define victim and/or author of cyberaggression is prone to error of underestimation of cyberaggression authors/perpetrators; this should be improved in future research. Finally, the study was a cross-sectional design; such an approach makes it difficult to investigate causal relationships between risk factors and online aggression. Longitudinal approach would be more appropriate in this context, echoing what has been done by You & Ah Lim (2016) among Korean middle school students.

Based on our findings the following are some of the main recommendations that can help reduce the prevalence of online aggression among university students in the Republic Democratic of the Congo. First, parents should have open communications with their children about Internet usage and cyberaggression; they should also suggest them to limit time presence on Internet and social media networks. Second, Universities and colleges should regularly organize meetings, forums and conferences around the dangers of Internet and set up concrete measures to mitigate risk of online aggressions between students. Finally, professors and lecturers should have time in their teaching programs to talk students about cyberaggression.

REFERENCES

Alvarez-Garcia, D. et al. (2015). Risks factors associated with cybervictimization in adolescence. *International Journal of Clinical and Health Psychology,* Vol. 15, Issue 3, pp. 226-235.

Alvarez-Garcia, D., Barreiro-Collazo, A., & Nûnez Pérez, J. C. (2017). Cyberaggression among Adolescents: Prevalence and gender Differences, Comunicar, Vol. XXV, No. 50.

Antipina, S., Bahkvalova, E., & Miklyaeva, A. (2020). Psychological Determinants of *cyber-aggression in institutionalized adolescents*. https://ceur-ws.org/Vol-2813/rpaper31.pdf

Athanasiades, C. et al. (2016). The "net" of the Internet: Risk factors for cyberbullying among secondary-school students in Greece. *European Journal on Criminal Policy Research*, Vol. 22, pp. 301-317. https://doi.org/10.1007/s10610-016-9303-4

Baldwin, M. et al. (2015). An examination of Cyber-Bullying and social media use in Teens: Prevalence, Attitudes and Behavior. *Journal of Bullying and Social Aggression*, Vol. 1 (1).

Bauman, S. (2009). Cyberbullying in a rural intermediate school: An exploratory study. *Journal of Early Adolescence*, Vol. 30 (6), pp. 803-833.

Bauman, S., & Baldasare, A. (2015). Cyberaggression among college students: Demographic Differences, Predictors, and the Role of the University. *Journal of College Students Development*, Vol. 56 (4), pp. 317-330.

Beyazıt, U., Simsek, S., & Aynur Bütün, A. (2017). An examination of the predictive factors of cyberbullying in Adolescents. *Social Behavior and Personality: An international Journal*, Vol. 45, pp. 1511-1522. https://doi.org/10.2224/sbp.6267

Blaya, C. (2011). Cyberviolence et cyberharcèlement: Approches sociologies. *La Nouvelle Revue de l'adaptation et de la scolarisation*, 2011/1, No. 53, pp. 47-65.

Blaya, C. (2013), *Les ados dans le cyberespace, Prises de risque et cyberviolence*, Pédagogies en développement, De Boeck Supérieur.

Blaya, C. (2015). Etude du lien entre cyberviolence et climat scolaire: Enquête auprès des collégiens d'Ile de France. *Les Dossiers des Sciences de l'Education*, Vol. 33, pp. 69-90.

Brewer, G. & Kerslake, J. (2015). Cyberbullying, self-esteem, empathy and loneliness. Computers in Human Behavior, Vol. 48, pp. 255-260. https://doi.org/10.1016/j.chb.2015.01.073

Çakır, Ö., Gezgin, D. M., & Ayas, T. (2016). The Analysis of the relationship between being a cyberbully and cybervictim among adolescents in terms of different variables. *International Journal of Progressive Education*, Vol. 12, Issue 3, pp. 134-154.

Chang, F. et al. (2015). Online gaming and risks predict cyberbullying perpetration and victimization in adolescents. *International Journal of Public Health*, Vol. 60, pp. 257-266. doi: 10.1007/s00038-014-0643-x

Chen, L. et al. (2016). A meta-analysis of factors predicting cyberbullying perpetration and victimization: From the social cognitive and media effects approach. New Media & Society, Vol. 19(8), pp.1194-1213 (https://doi.org/10.1177/1461444816634037).

Cho, S. et al. (2019). Social-ecological correlates of cyberbullying victimization and perpetration among African American youth: negative binomial and zero-inflated negative binomial analyses. *Children and Youth Services Review*, Vol. 101, pp. 50-60. https://doi.org/10.1016/j.childyouth.2019.03.044

European Parliament (2016). Cyber Bullying among Young People. *Study for the LIBE Committee, PE 571.67*. https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2016)571367

Even, C. (2019). Cyberharcèlement chez les adolescents: Impacts psychopathologiques, émotionnels et cognitifs. *Revue de littérature, Médecine humaine et pathologie*, 2018. https://dumas.ccsd.cnrf.fr/dumas-02014346

Festl, R. & Quandt, T. (2016). The role of online communication in long-term cyberbullying involvement among girls and boys. *Journal of Youth and Adolescence*, Vol. 45, pp. 1931-1945. doi: 10.1007/s10964-016-0552-9

Finkelhor, D. et al. (2000). Online Victimization: A Report on the Nation's Youth. *National Center for Missing & Exploited Children*, 2000. https://www.unh.edu/ccrc/sites/default/files/media/2022-03/online-victimization-a-report-on-the-nations-youth.pdf, juin 2000

Gozlan, A. (2018). Quand l'altérité devient virale : exemple de cyberbullyin, Savoirs et Cliniques, Volume I (24), pp. 165-173.

Hashima, P. & Finkelhor, D. (1999). Violent victimization of youth versus adults in the National Crime Victimization Survey. *Journal of Interpersonal Violence*, Vol. 14 (8), pp. 799-819.

IGI Global, (n.d.) *InfoSci-Dictionary*, https://www.igi-global.com/e-resources/infosci-databases/infosci-dictionary/, consulted at 19/02/2023

Larrañaga, E., et al. (2016). Loneliness, parent-child communication and cyberbullying victimization among Spanish youths. *Computers in Human Behavior*, Vol. 65, pp. 1-8. https://doi.org/10.1016/j.chb.2016.08.015

Lee, C. & Shin, N. (2017). Prevalence of cyberbullying and predictors of cyberbullying perpetration among Korean Adolescents. *Computers in Human Behavior,* Vol. 68, pp. 352-358. https://doi.org/10.1016/j.chb.2016.11.047

Les études du Centre Jean Gol, (2017). *Le cyber–harcèlement des enfants et des adolescents*. https://www.cjg.be

Li, Q. et al. (2020). Risk factors of cyberbullying perpetration among school-aged children across 41 countries: a perspective of routine activity theory. *International Journal of Bullying Prevention*, Vol. 3, pp. 168-180. https://doi.org/10.1007/s42380-020-00071-6

Macilotti, G. (2019). Violence et humiliation à l'ère numérique: Une étude en milieu scolaire. *Médecine et Hygiène*, Vol. 43, pp. 299-328.

Malinowska-Cies'lik, M., Dzielska, A., & Oblacin'ska, A. (2022). Psychosocial Determinants of Adolescents 'cyberbullying involvement – The role of body satisfaction. *International Journal of Environmental Research and Public Health*, Vol. 19 (3). https://doi.org/10.3390/ijerph19031292

Marin-Cortés, A. et al. (2019). Risk and protective factors related to cyberbullying among adolescents: a systematic review, Psychologist Papers, Vol. 40 (2), pp. 109-124.

Mbaki Luzayisu, E. & Zamwangana Tungu, J.P. (2023). Cyberagression chez les étudiants en République démocratique du Congo (DRC). *Essai de mesure et d'identification de facteurs de risque, Survey Report*, Kinshasa.

McCrae, R. R. & Costa, P. T. (1987). Validation of the five-factor model of personality across instruments and Observers. *Journal of Personality and Social Psychology*, Vol. 52, No. 1, pp. 81-90. https://doi.org/10.1037/0022-3514.52.1.81

Mendez-Baldwin, M. et al. (2015). An examination of cyber-bullying and Social media use in Teens: prevalence, attitudes and behaviors. *Journal of Bullying & Social Aggression*, Vol. 1 (1). http://sites.tamuc.edu/bullyingjournal/article/cyber-bullying-among-teens/

Menesini, E. et al. (2012). Cyberbullying Definition Among Adolescents: A comparison Across six Europeans Countries. *CyberPsychology, Behavior and Social Network*, Vol. 15, No. 9, pp. 455-463. https://doi:10.1089/cyber.2012.0040.

Merril, R. & Hanson, C. (2016). Risk and protective factors associated with being bullied on school property compared with cyberbullied. *BMC Public Health*, Vol. 16 (145). doi: 10.1186/s12889-016-2833-3.

Mishna, F. et al. (2010). Exploring factors associated with cyberbullying among middle and high school students. *American Journal of Orthopsychiatry*, Vol. 80, No. 3, pp. 362-374.

Mitchell, B. A. (2003). Life Course Theory. In J. Ponzetti (ed.), *The International Encyclopedia of Marriage and Family Relationships*. Macmillan Reference, New York, pp. 1051-1055.

Palermiti, A. et al. (2017). Cyberbullying and self-esteem: An Italian study. *Computers in Human Behavior*, Vol. 69, pp. 136-141. https://doi.org/10.1016/j.chb.2016.12.026

Park, S., Na, E. Y., & Kim, E.-M. (2014). The relationship between online activities, netiquette and cyberbullying. *Children and Young Services Review*, Vol. 42, pp. 74-81. https://doi.org/10.1016/j.childyouth.2014.04.002

Peker, A. (2015). Analyzing the risk factors predicting the cyberbullying status of secondary school students. *Education and Science,* Vol. 40 (181), pp. 57-75. doi: 10.15390/EB.2015.4412

Petrosyan, A. (2022). *Internet penetration rate in the European Union from 2019 to 2022, by country*. https://www.statista.com/statistics/1246141/eu-internet-penetration-rate

Rosenberg, M. (1965). *Society and the Adolescent Self-Image.* Princeton University Press: Princeton.

Runions, K. et al. (2018). Disentangling Functions of Online Aggression: The Cyber-Aggression Typology Questionnaire (CATQ). *Agressive Behavior,* Vol. 43 (1).

Sasson, H. & Mesh, G. (2017). The role of parental mediation and peer norms on the likelihood of cyberbullying. *The Journal of Genetic Psychology,* Vol. 178 (1), pp. 15-27. doi: 10.1080/00221325.2016.1195330

Smith, P. K. et al. (2008). Cyberbullying: its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*. Vol. 49 (4), pp. 376-385.

Stahel, L. & Weingartner, S. (2019). Online aggression from a sociological perspective: An integrative view on determinants and possible countermeasures. *Proceedings of the Third Workshop of Abusive Language Online*. Florence, Italy, Association for Computational Linguistics, pp. 181-187.

Tisseron, S. (2003). Le désir "d'extimité" mis à nu. *Le Divan familial*, Vol. 11 (2), pp. 53-62.

UNICEF (2019). UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying. *U-Report highlights prevalence of cyberbullying and its impact on young people*. https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying

UNICEF (n.d.). *Cyberbullying: What is it and how to stop it*. https://www.unicef.org/end-violence/how-to-stop-cyberbullying#2

Vale, A. et al. (2018). Cyber aggression in adolescence and internet parenting styles: a study with victims, perpetrators and victim-perpetrators. *Children and Youth Services Review*, Vol. 93, pp. 88-99.

Wright, M. (2017). Parental mediation, cyberbullying, and cybertrolling: The role of gender. *Computers in Human Behavior*, Vol. 71, pp. 189-195. https://doi.org/10.1016/j.chb.2017.01.059

You, S. & Ah Lim. S. (2016). Longitudinal predictors of cyberbullying perpetration: Evidence from Korean middle school students. *Personality and Individual Differences*, Vol. 89, pp. 172-176. https://doi.org/10.1016/j.paid.2015.10.019

Yusuf, S. et al. (2021). Cyberaggression – Victimization among Malaysians Youth. *Asian Journal of University Education*, Vol. 17, No. 1, pp. 240-260.

Zang, Y. et al. (2021). Parenting Style and Cyber-Aggression in China Youth: The Role of Moral Disengagement and Moral Identity. *Frontiers in psychology*, Vol. 12, 621878.