Duality between E-commerce and Cybersecurity: Case of Central Africa

ABSTRACT

In this article, the duality between e-commerce and cybersecurity in Central Africa's case has been presented. To achieve this, a field study was conducted by submitting a question in order to make sure that the impact of cybersecurity on e-commerce in Africa in general and Central Africa in particular is real. A questionnaire was submitted to small and medium-sized business online sales companies, Congolese campuses, research laboratories, those who submit the articles online, and African Internet users. Risk assessments based on loopholes, threats, and countermeasures were also conducted. The results of this study are successful insofar as the results of the survey sufficiently prove the existence of the problem. The outcome of the risk assessment based on flaws, threats, and countermeasures is the panacea for the investigation, in the sense that strengthening countermeasures at the level of online merchants minimizes the risk of being attacked or victimized.

Keywords: Cybersecurity, E-commerce, Modeling.

1. INTRODUCTION

Since the advent of the Internet, e-commerce systems have guaranteed a large number of customers, who continue to use these systems with increasing orders placed electronically and deliveries made without geographical limits [**1**]. These systems improve normal trade flows, like today's e-commerce transactions between businesses and customers, businesses and customers, and so on. A survey of customers' online shopping habits reveals that more than 5,000 customers will make at least two online purchases in a three-month period [1]. However, the ease introduced by e-commerce solutions has also come with serious cyber threats to the system. Africa is one of the continents that is still on the margins of development in terms of cybersecurity, so according to the British consulting firm, one billion people in Africa should have access to the internet in 2022 [**2**]. And today, with the arrival of the internet and the increase of the economic crisis in African countries in general and in Congo Brazzaville in particular, Congolese youth, having passed a number of training courses on e-commerce, are active in the e-commerce of a number of products, such as artificial hair, a trade widely practiced by Congolese students residing on university campuses. Added to this are teacher-researchers and doctoral students who are involved in research, and the latter submit their research work online. But the latter face many difficulties in the online communication process, as

data is often intercepted by hackers and many other ill-intentioned people. Not to mention the young people who exchange cash for electronic money, what we vulgarly call mobile money; these too are confronted with electronic theft in the process of sending or receiving money. In this article, we present the duality between e-commerce and cybersecurity in Central Africa, based on the case of Congo-Brazzaville. This study will be based on a survey, in the case of data collection, of those who do e-commerce and those who make others exchange money on the Internet. In a second step, we will assess the risks of a network or an individual being attacked on the Internet based on threats, flaws, and countermeasures. A current solution would be public awareness and training for all those who engage in electronic activities.

1. Positioning the problem

E-commerce is the exchange of goods and services for money or other forms of payment on the cloud. It can be carried out in a metropolitan network or in a wide-area network. E-commerce businesses are increasingly using cloud services to save money, but they don't always ensure that the services use strong online security measures. This combination of cloud services and a lack of robust online security offers the hacker the ability to easily access tons of sensitive data [**3**]. However, online businesses, such as Amazon, Ali Baba, and many others, can realize substantial benefits and increase potential additional revenue streams by taking steps to mitigate customer fears, such as using technology to protect sensitive customer data, authenticate their websites, and build consumer trust [**3**].

In Africa, there is the free trade area, which represents a trading bloc where member countries sign a free trade agreement to keep few or no barriers to trade in the form of tariffs (tariffs) or quotas between them. This agreement generally includes cooperation between countries to reduce non-tariff barriers to trade and increase trade between them. For example, ECOWAS manages a free trade area in which tariffs on intra-regional imports have been eliminated for goods that meet the rules of origin; this theme had already been pinpointed just before the COVID-19 pandemic in the context of the definition of a regional strategy converging on mechanisms for minimizing online attacks [**4,5**].

African trade is often hampered by problems related to logistics, trade finance, or regulations. Logistics costs in Africa are three to four times higher than the global average [**4**]. Africa's trade finance gap, roughly measured by the total value of trade finance applications rejected by banks, stood at USD 81.8 billion in 2019, limiting the ability of African producers to compete in international markets. Similarly, cross-border payments in Africa are often costly.

.

2- Current status

Cloud computing allows today's small and medium businesses and their employees to work from anywhere, anytime, using multiple devices. They can transfer files using Drop Box, video conference globally with Skype and other sites, and access work remotely from their smartphones and tablets [5,**6**]. But as some small businesses have painfully learned, the price of these collaborative benefits is the potential for a serious data security breach. If small businesses have Fortune 500 customers, they provide an easy entry point to a much larger trove of data. Businesses of all sizes must assume a state of compromise today because failure to do so can result in significant costs from lost data or theft of intellectual property, disruption of business operations, and damage to the company's reputation, which can lead customers to turn to the competition. All businesses need to assess their cybersecurity weaknesses so they can develop a strategy to protect sensitive data. A basic question to ask is: what is the most sensitive data for the company? A pharmaceutical company may have the formula for a new drug stored in a document stored securely on its hard drive, but the data has also been shared by researchers via email without encryption. Similarly, government and non-profit agencies have large amounts of sensitive taxpayer data on file, which is loaded onto employee laptops or USB drives for business purposes without encryption. It is important to ask specific questions about how the data is recorded and transported, what media are used to store the data, where the data originated, and who gained access to the networks. The most valuable data for a hacker may not reside in the company's own database, but it may provide access to its customers [**6**].

Answering these questions is essential for effective cybersecurity risk management. Some small and medium-sized businesses have started using "penetration testers" to test the strength of their defenses. However, they find that these "counterintelligence" measures need to be constantly updated to stay ahead of thieves in the cybersecurity game **[7].** One such technique is to sacrifice some of the convenience of integrated data and keep sensitive information in separate groups. Such a strategy will require careful consideration of the information needs of managers as well as the definition and application of rules for information sharing. Another technique used by counterintelligence experts is to offer tempting targets as "honeypots" to lure attackers and allow their movements to be monitored **[8]**. This technique is actually used by certain banking establishments, which can alert the police. A successful security system design should include a checklist of preventive, detective, and corrective steps to increase the chances of successful security system design and implementation. Here are some examples: Preventative: **[9]** understand the computer and network security landscape; (2) put in place the basic safeguards. Detectives [9] identify security threats; **[10].** identify security measures and their application. Fix: Clapper et al. understand computer emergency response team services;**[10].** prepare a comprehensive security system; and Bidgoli et al. plan for business continuity. Whatever the strategy, managers need to develop "constructive paranoia" and start thinking about ways to breach the data. They must always be alert to unusual incidents or patterns and follow security protocol without fail. The primary reason for small businesses' failure to invest in cybersecurity appears to be the misconception that such an investment is a discretionary expense item and a failure to understand that it is an essential defensive cost to stay alive. Studies **[11]** have shown that 89% of consumers avoid companies that fail to protect

UNDER PEER REVIEW

their privacy online, as evidenced by declining sales at companies like Target and Home Depot. Business partners also require proof that their interests and privacy are protected. Adequate security has become a requirement for companies to collaborate or outsource work. 54% of US companies have basic standards that they expect from their external partners, suppliers, and vendors **[11].**

While small businesses lack the resources and time to research the most appropriate cybersecurity tools, a "one-size-fits-all" approach to cybersecurity by installing the best-selling package is not the solution. Businesses need to adopt new risk management strategies that focus more on the consequences of a wide range of potential risk events and less on the likelihood of the events occurring. New threats related to trends in globalization, rapid technological change, and the realignment of economies are increasing market volatility and disrupting thinking about "black swan events", i.e., low probability events with high impact. For small businesses that don't change their risk management by viewing security breach events as "black swans," this can pose the greatest risk to their strategy and future growth. They need to review their current risk management approach and decide if this can get them to the desired future state. This may require a shift in mindset to view risk management as a business enabler that helps propel the organization forward, rather than a rigid structural shield **[12].**

3- Literature review

3.1. Ecommerce

E-commerce is a growing field that has come into being due to the advancement and convergence of technology and the Internet, where people do many commerce-related activities. In other words, e-commerce refers to selling and buying products online. It is an online money transfer in exchange for completing trade activity. Electronic commerce uses digital means to develop and carry out different actions and transactions between organizations or groups or between a company and a customer. According to one study, there are more than 12 to 24 million e-commerce sites across the globe [**13**]. Figure 1 shows the breakdown by country of online sales in 2021 **[14].** In e-commerce, the business process of buying and selling is completed with the help of the internet. Important e-commerce activities include the selection of a specific product, money transfer, and data exchange [**16**]. Other activities include Internet marketing, online management systems, and automatic data collection systems.

E-commerce helps businesses by expanding their market reach and size and reducing operating costs and barriers **[17].** Research shows that it has a positive impact on the economy **[17].** In e-commerce, a customer buys directly from the online store using mobile apps and websites. Communication can take place via chatbots, live chat, or voice assistants. Figure 2 **[18]** below summarizes the framework of a customer's e-commerce business process. The world is shifting from in-store shopping to online shopping, and big companies like Alibaba, Amazon, etc. are leading the transition. Due to this change, technological advancements are affecting other online business processes **[19].** E-commerce makes it easy for

customers to buy something and has also been shown to be one of the most powerful agents for business transformation **[20].** The market value of e-commerce in 2021 is given in the following figure 3. It shows that Amazon has the largest share, worth USD 1.634 billion [**15**]. Due to rapid growth, companies have upgraded their networks, operations, etc. to better serve suppliers and customers. Yesterday's e-commerce technology made impossible goals for possible business enterprises by providing them with many opportunities to find and conquer new markets and attract customers across borders **[20].** Although e-commerce has many advantages for companies and customers, it is impossible without a sophisticated approach to security [**21**]. There are four main market segments in which e-commerce operates. These sections are Business to Business, where the sale of products is between businesses; Business to Consumer, which involves sales between businesses and consumers; Consumer to Consumer, which enables sales between individuals; and Consumer to Business, where individuals sell to businesses [**22**]. It is important to note that in 2020, e-commerce sales were 4.28 billion USD and are expected to reach 5.4 billion USD. The share of e-commerce was only around USD 469.2 billion in the United States in 2021. Figure 2 below shows e-commerce statistics from 2014 to 2024 [**23**]. Trends and statistics show that e-commerce is an area of doing business that is not limited to some specific areas.

REVIEW

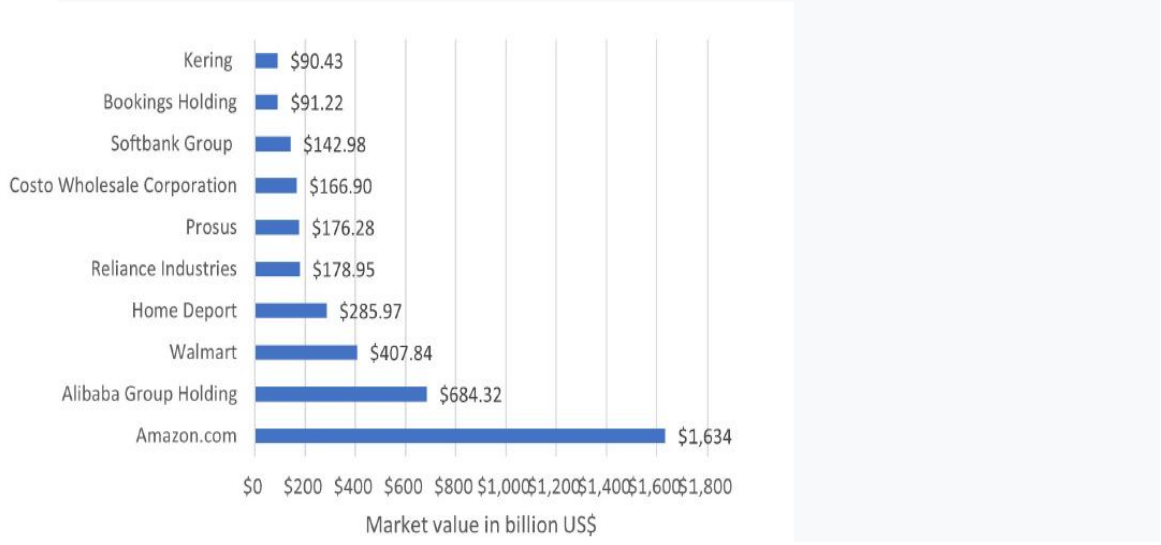


Figure1: Top e-commerce companies by market value [15].

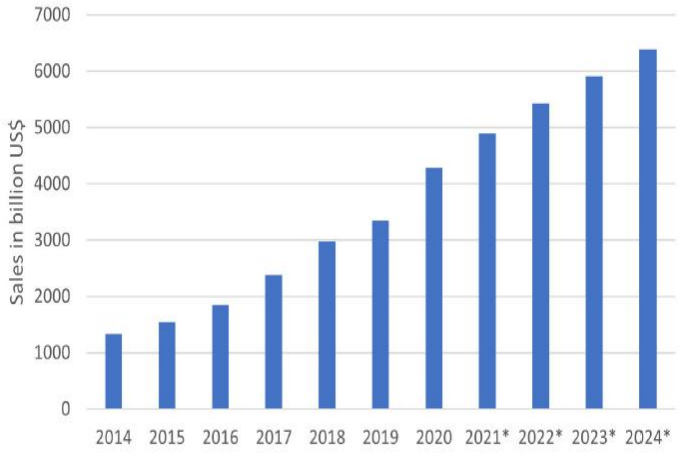


Figure 2: E-commerce sales worldwide [23].

This is typical where the internet and technology are available across the globe. For example, an industry like tourism is also adopting technology and changing its traditional business. Now the sale and purchase of tickets, hotel reservations, etc. can be done with the help of the internet and relevant technology. The market size of the global online travel agent industry is approximately USD 432 billion, the global online travel booking platform industry is approximately USD 517 billion, and the share of online sales revenue in travel and world tourism accounts for approximately 65%. Therefore, technology and e-commerce companies must be able to conduct business smoothly and provide their customers with the best possible experience. But as said earlier, as technology is involved between buyers and shoppers, the activity ends remotely after sharing the required information. E-commerce invites many threats, and cybersecurity is the most common and severe [**23**].

4- Some general information on cybersecurity

Computer security is the set of measures implemented to reduce the vulnerability of a system against accidental or intentional threats. The objective of computer security is to ensure that the hardware and/or software resources of a computer park are only used within the framework provided and by authorized persons [**24**]. It is necessary to identify the fundamental requirements in computer security, which characterize what users of computer systems expect with regard to security [**24**].

- **Confidentiality**: Only authorized persons should have access to the data. Any interception must not be able to succeed; the data must be encrypted, and only the actors of the transaction have the key to understanding [**24**]
- **Integrity**: It must be guaranteed at all times that the data circulating is those that we believe and that there has been no alteration (voluntary or not) during the communication. Data integrity must validate data completeness, accuracy, authenticity, and validity [**24**].

- **Availability**: It is necessary to ensure the proper functioning of the system and access to services and resources at any time. The availability of equipment is measured by dividing the time during which this equipment is operational by the time during which it should have been operational [**24**].
- **Non-repudiation:** A transaction cannot be denied by any of the correspondents. The non-repudiation of the origin and receipt of the data proves that the data was indeed received. This is done through digital certificates using a private key [**24**].
- **Authentication**: It limits access to authorized persons. It is necessary to ensure the identity of a user before the exchange of data.

5- Risk modeling in a computer network

As we said in this research work, we will focus on assessing the risks that a subscriber or user may run during online exchanges. In fact, with the development of the use of the Internet, many companies open their information systems to their partners or suppliers; they are more at the level of the three-tier or n-tier architecture. It therefore becomes necessary to know the company's resources to be protected and to control access control and the rights of system users. On the other hand, security is a compromise between costs, risks, and constraints. We will better understand the weight of a risk by relying on the following formula [**24**]. To do this, we model the risks using the following formula:

$$R = \frac{M \times V}{C} \qquad (1)$$

Where R is the probability of a threat exploiting a vulnerability. In other words, there is a possibility that a harmful event will occur.

M: is the threat, i.e., the danger (internal or external), such as a hacker, a virus, etc.

V: is the vulnerability, that is to say, a weakness inherent in a system (software or hardware). Sometimes called a fault or breach, it represents the level of exposure to the threat in a particular context.

C: for countermeasure, it is the means allowing to reduce the risk in an organization; note that the risk is all the more reduced as the countermeasures are numerous, and it is more important if the vulnerabilities are numerous [**24**].

6- Results and discussion

6.1. Results of a first survey carried out in the field in 2021.

The results in Table 1 below represent the results obtained in the field; we conducted a survey of e-commerce subscribers. To do this, we submitted them a questionnaire, which consisted of knowing the probability that they had been the victim of a computer attack. So, to answer this question, we have chosen, as samples, the SMB (Small and Medium Business)

UNDER PEER REVIEW

Table 1: Result obtained in the field.

Parameters	SMB	Marien NGOUA BI University	INTERNET USERS	Campus of the Marien Ngouabi University	RESEARCHERS AND RESEARCHERS' TEACHERS
n	18	255	1500	11	850
x	11	242	1003	8	301
y	8	201	1100	7	250
z	11	198	855	6	745

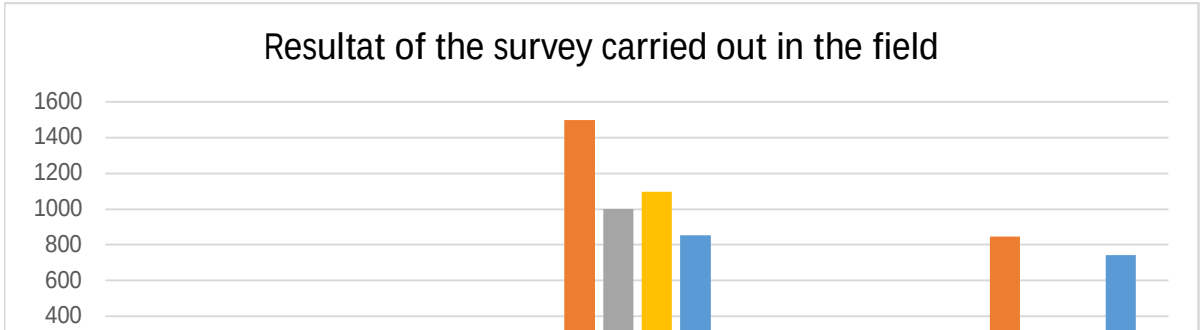
UNDER PEER REVIEW

Where n is the parameter that represents the number of people we contacted in relation to the sector of activity.

x: people who responded positively to our questionnaire

y: those who carry out an online business or who have a relative who does an electronic activity.

z: those who were victims or who have a relative who was a victim of the cyberattack.



REVIEW

Figure3: Results of the field carried out from 2019 to 2021

The graph in Figure 3 represents the results of the survey carried out as part of the evaluation of the influence of cybersecurity in Africa in general and in the Congo in particular. Given the absence of many companies in the Congo, we are therefore focused on small and medium-sized enterprises (SMBs), academia, campuses, research laboratories, and Internet users. It should be noted that it is at the level of Internet users that there is more impact; this is very often due to the hacking of Facebook and WhatsApp accounts and many others. In the vast majority, those who do e-commerce from Congo to China and Dubai are victims of attacks, hacking of email addresses, and making payments of money to other people believing that they communicate with sellers. It should also be noted that at the level of researchers or teacher-researchers, Africans in general and Congolese in particular who submit articles or books online are often victims of fraud, either by the person who pretends to be a publisher in chief or by the person who pretends to be a publisher in chief, and after the transaction of money until the period when the article is supposed to be examined, the connection with the editor is often blurred. This same problem is observed at the level of students residing in the Congolese camps, who are used to doing small business locally and internationally and are often victims of chopping.

6.2. Results of a second survey carried out in the field in 2022.

We conducted this second survey in the context of the electronic commerce of money and telephone credit in the networks of MNT Congo and Airtel Congo. We have thus put in a questionnaire to find out if the subscriber or user of this service has already been a victim of online transactions, or what we commonly call mobile money. The results of this survey are shown in Table 2 below:

Table2: **Result obtained in the field for the second scenario**

Parameters	Students	Civils servants	Phoneboxes owners	Random people	Sellers
x	1850	450	301	2500	1523
y	1781	404	280	2421	1431
z	802	151	258	1985	1340
t	433	123	250	1503	1301

Where:
x: respondents
y: those who agreed to answer
z: those who have been attempted a cyberattack
t: those who have been victims of attacks

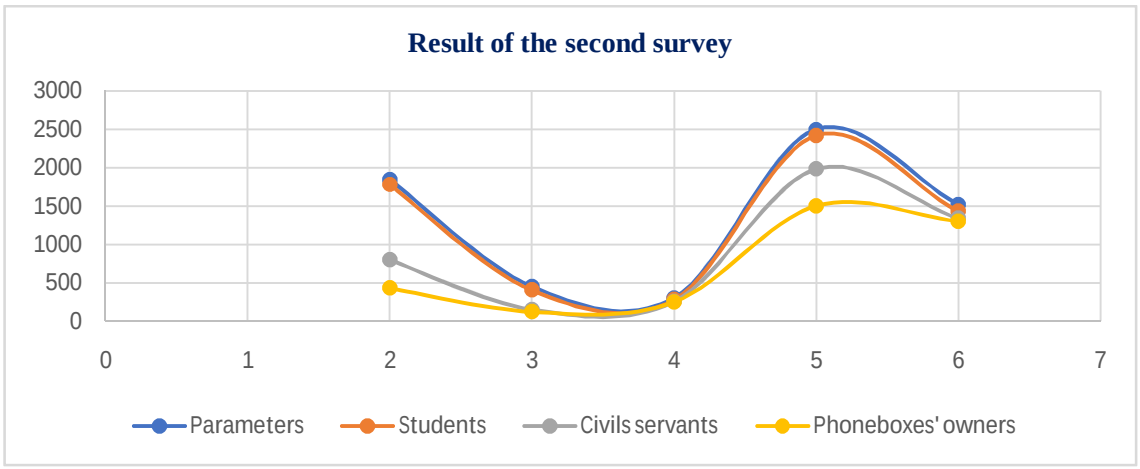


Figure 4: Results of the survey conducted in the city of Brazzaville and Pointe Noire.

The graph in Figure 4 represents the results of the survey conducted in the cities of Brazzaville and Pointe Noire as part of assessing the possibility of a person

being the victim of an attack in electronic money exchanges. It should be noted that in these curves, those who are more victims are those who work in the exchange telephone booths. By questioning them, on the reason for this frequency of scam, they said that it is the fact of returning the telephone to the customers that the latter make compositions of the figures which go as far as withdrawing money from them.

6.2. Results of risk simulations based on countermeasures.

In the relationship of formula (1), we have defined the risk for a network or a person to be vulnerable or attacked. It should be noted that in this formula, it is the countermeasures that vary according to the product between the threats and vulnerability. These different parameters are defined according to the faults likely to occur in a network. In cases of IP spoofing, which refers to IP address spoofing, it is made to believe that the request comes from an authorized machine. A good configuration of the entry router prevents an external machine from pretending to be an internal machine. This case occurs a lot in the cases of small and medium enterprises when exercising electronic commerce on the internet.

Table 3. Different values obtain from the network that we use for simulation

Risk	Threats	Vulnerability	Countermeasures
0,1 0,2 0,3 0,4	10 6 2 4	5 3 1 2	4 3 2 1

UNDER

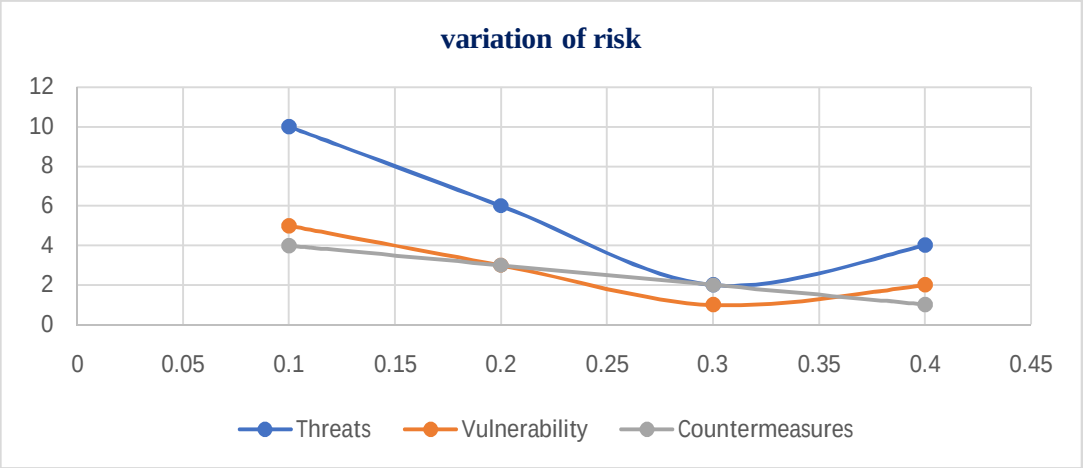


Figure 5: Result of risk simulation according to threats, flaws and countermeasures.

This graph represents the variation of IT risk according to threats, vulnerabilities, and countermeasures. It should be noted that more threats or vulnerabilities relating to IP spoofing, which refers to the spoofing of IP addresses; DNS spoofing, which refers to the DNS server accepting the intruder; massive flooding of unterminated connections; smurfing, which represents bandwidth saturation; the hoax, which refers to the rumor that is transmitted by email; the hacker and cracker; and the sniffer, which refers to listening to the network, increase the risk that the network or the individual who carries out the electronic commerce is attacked. The solution in this case is to strengthen the countermeasures so that the more they increase, the lower the risk of being victims. These simulations refer to a model that we have proposed, establishing a relationship between faults and threats. We told ourselves that flaws and threats are interdependent, which allowed us to write: flaws = k*threats, where k is a positive constant and not zero.

Conclusion

Throughout this study, we have tried to demonstrate first of all the positioning of the problem on the international level, first in the case of Africa in general and the case of central Africa in particular, but most of our focus was on the Congo. Brazzaville case. The status of the problem was also presented. We also did a bibliographical review relating to the resolution of the theme in the literature. The results that we obtained about the duality between e-commerce and cybersecurity allow us to conclude that there is awareness among the African population, in student circles, in the teams of teacher-researchers who submit articles online, and among other people who do e-commerce through a computer network or through their cell phones. A good configuration of the entry routers will prevent an external

machine from pretending to be an internal machine. The separation of the DNS of the LAN from that of the public space, the activation of the firewall, or the distribution of the servers would be a better way to reinforce the security of a network. Beware of social engineering, especially those who impersonate, who can be described as hackers, and who seek to obtain confidential information from company personnel for future intrusion. Only staff training can protect against such an attack. The results we obtained in the two scenarios are encouraging. Strengthening countermeasures to secure themselves in a network or individually would be an essential solution to minimize the risk of attacks. Given the limitations of this study, we were unable to analyze all of this very broad topic in our data collection. However, it would seem interesting to us in the future to explore the attack interception system automatically.

UNDER PEER REVIEW

COMPETING INTERESTS DISCLAIMER:

Authors have declared that they have no known competing financial interests OR non-financial interests OR personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] Fortune. Consumers Are Now Doing Most of Their Shopping Online. 2018 [online] Available at: http://fortune.com/2016/06/08/online-shopping-increases/ [Accessed 5 Mar. 2018].

[2] Kshetri, Nir (2019). "Cybercrime and Cybersecurity in Africa," Journal of Global Information Technology Management. DOI: 10.1080/1097198X.2019.1603527, 2019.

[3] Kamala Raghavan1, Mayur S. Desai, P.V. Rajkumar « Managing Cybersecurity and e-Commerce Risks in Small Businesses »2021

[4] **Alessandro Vitale**, Laura **Cyron**, **Cécile Barayre** et **Torbjörn Fredriksson**.United Nation « Conférence des nations unies sur le commerce et le développement », publications@un.org ; Web site : https://shop.un.org ;2022

[5] Affia, Abasi-amefon Obot "Security Risk Management of E-commerce Systems", Tartu 2018

[6] Bidgoli, Hossein. 2016. Integrating Real Life Cases into A Security System: Seven Checklists For Managers, American Journal of Management, 16 (4) :9-25.

[**7**] Schumpter, Joseph. Aug 2015. "Manage like a Spymaster" (http://www.economist.com/news/business/21662540-counter-intelligence-techniques-may-help-firms-protect-themselves-against-cyber-attacks-manage) – Accessed on Sept 7, 2015.

[**8**] Martin, William W, 2001. “Honey Pots and Honey Nets - Security through Deception”. Available at 25http://www.sans.org/reading-room/whitepapers/attacking/honey-pots-honey-nets-security-deception-41 SANS Institute InfoSec Reading Room, CISSP May - Accessed on September 7, 2015
[9] Clapper, Danial, and W. Richmond. 2016. Small business compliance with PCI DSS, Journal of Management Information and Decision Sciences, 19 (1):54-67.
[10] Lanz, Joel. 2014. “Cybersecurity governance: the role of the audit committee and the CPA”. The CPA Journal, November: 6-10.
[11] PwC. 2012. Cyber Security: Why you can’t afford to ignore it, Growing Your Business PwC.
[**12**] Abasi-amefon O. AFFIA1, Raimundas MATULEVICIUS ˇ 1, Alexander NOLTE1,2 “Security Risk Management in E-commerce Systems: A Threat-driven Approach,”2020.
[13] Gennaro, L. (2022). 68 Useful ecommerce statistics you must know in 2022. Available online at: https://wpforms.com/ecommerce-statistics/ (accessed April 1,2022).
[14] OBERO (2022a). E-commerce Sales by Country. Available online at: https:// www.oberlo.com/ (accessed April 20, 2022).
[15] OBERO (2022b). Top ecommerce companies. Statistics. Available online at: https: //www.oberlo.com/ (accessed April 20, 2022).
[16] Lorette, K. (2022). How ecommerce can reduce business transaction costs. Small business. Available online at: https://smallbusiness.chron.com/adobe-creativecloud- grow-business-13771091.html (accessed April 13, 2022).
[17] Anvari, R. D., and Norouzi, D. (2016). The Impact of E-commerce and R&D on economic development in some selected countries. Proc. Soc. Behav. Sci. 229, 354–362. doi: 10.1016/j.sbspro.2016.07.146.
[18] Smart Draw (2022). E-commerce workflow diagram. Available online at: https: //www.smartdraw.com/ (accessed March 2, 2022).
[19] Hooks, D., Davis, Z., Agrawal, V., and Li, Z. (2022). Exploring factors influencing technology adoption rate at the macro level: A predictive model. Technol. Soc. 68:101826. doi: 10.1016/j.techsoc.2021.101 826
[20] **Yu Zheng [a], Zheng Li [a], Xiaolong Xu [a b], Qingzhan Zhao [c]** “Dynamic defenses in cyber security: Techniques, methods and challenges” August 2022.
[21] Dupont, B. (2012). The cyber security environment to 2022: Trends, drivers and implications. Available online at: https://ssrn.com/abstract=2208548 (accessed February 20, 2022).

[22] Shopify (2022). Ecommerce. Encyclopedia/what-is-ecommerce. Available online at: https://www.shopify.com/ (accessed April 1, 2022).

[23] Statista (2022). Retail e-commerce sales worldwide from 2014 to 2024. Available online at: https://www.statista.com/statistics/379046/worldwide-retaile-commerce-sales (accessed April 20, 2022).

[24] Dr YENDE RAPHAEL Grevisse, 2KABIENA KABASELE Emmanuel, 3MUKENDI MALUNDA Cedrick,4KATAYI NTUMBA Freddy, et5 LOWEMBO A TSHOTSHO Raymond « Mise en place d’un système sécurisé de télé-administration dans un réseau local d’entreprise : Application simulée aux
UNDER PEER REVIEW

institutions universitaires en ville de KANANGA (RDC) » Journal homepage: www.ijrpr.com ISSN 2582-7421.

UNDER PEER REVIEW