Scientific Research Publishing

Journal of Computer and Communications, 2023, 11, 12-32
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

The Knowledge of Cyber-Security Vulnerabilities in an Institution of Higher and University Education. A Case of ISP-Bukavu (Institut Supérieur Pédagogique de Bukavu) (TTC = Teachers' Training College)

Dominique Wasso Kiseki[1], Vincent Havyarimana[2], Therence Niyonsaba[3], Désiré Lumonge Zabagunda[4], Walumbuka Ilundu Wail[5], Thabo Semong[6]

[1]Computer Engineering, University of Burundi (UB), Bujumbura, Burundi
[2]Ecole Normale Supérieure (ENS), Bujumbura, Burundi
[3]University Research Laboratory in Modeling and Applied Statistical Engineering (LURMISTA), Nyamugerera, Bujumbura
[4]Department of Physics and Technology ISP, Bukavu, Democratic Republic of Congo
[5]Department of Management Computer Science ISP, Bukavu, Democratic Republic of Congo
[6]Departement of Computer science and Information System, Bostwana International University of Science and Technology, Palapye, Bostwana
Email: wassokisekidom@gmail.com, havicent12@gmail.com, semongt@biust.ac.bw

How to cite this paper: Kiseki, D.W., Havyarimana, V., Niyonsaba, T., Zabagunda, D.L., Wail, W.I. and Semong, T. (2023) The Knowledge of Cyber-Security Vulnerabilities in an Institution of Higher and University Education. A Case of ISP-Bukavu (Institut Supérieur Pédagogique de Bukavu) (TTC = Teachers' Training College). *Journal of Computer and Communications*, **11**, 12-32.
https://doi.org/10.4236/jcc.2023.114002

Received: November 27, 2022
Accepted: April 21, 2023
Published: April 24, 2023

Abstract

This study pursues the objective of analyzing and verifying the knowledge of the agents of the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) in relation to the practical flaws resulting from the lack of knowledge of the observable rules in information system security. In a clearer way, it aims to verify the level of knowledge of the vulnerabilities, to verify the level of use of the antivirus software, to analyze the frequency of use of Windows update, the use of an anti-spyware software as well as a firewall software on the computer. Through a survey conducted on a sample of 100 agents of the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College), the results revealed that 48% of the sample has no knowledge on computer vulnerabilities; for the use of antivirus software: 47% do not use the antivirus; for Windows update: 29% never update the Windows operating system; for anti-spyware: 48% never use; for the firewall: 50% are not informed. In fine, our results proposed a protection model VMAUSP (Vulnerability Measurability Measures Antivirus, Update, Spyware and Firewall) to users based on the behavioral approach, learning how the model works.

Keywords

Threats, Vulnerabilities, Cybersecurity, Anti-Spyware, Firewall, Cyber-Attack, Antivirus

1. General Introduction

In the current context, the generalized opening and interconnection of computer networks facilitates the sharing of internal information between customers, suppliers and other partners [1]. With the advent of the digital era, several theories and techniques have been created, resulting in new forms of crime involving information systems. Malware unconditionally represents a real threat to the security of computer systems. Therefore, it seems vital for nations and institutions to have an updated legal system capable of effectively protecting users against any criminal behavior typical of this technological environment [2]. In the literature review, a study showed that the exploitation of a single basic computer vulnerability can damage the operational activities of an organization. Then, it deteriorates its image, it leads to a loss of trust towards partners, it decreases its value and eventually leads to its disappearance [3]. The development of information and communication technology has brought countless benefits to humanity. With the current technological changes, the Information and Communication Technologies (ICT) with the support of the Internet are transforming humanity from a traditional society into a modern society evolving through time [4]. However, despite these contributions, concerns persist to some degree and at different levels. Let us add that, besides the obvious advantages of the development of Information and Communication Technologies (ICT), several serious disadvantages have emerged. First of all, it was estimated that there are 4.77 billion active internet users, 4.17 billion unique holders of cell phones connected to the internet and 3.96 billion unique users of social networks [5]. This interconnection to the internet, which has become an essential place to consume, exchange and increase one's knowledge, could be one of the reasons for vulnerability. This trend is limited to Asia, Europe and North America, although there has been a strong progression in Africa and the Middle East in recent years.

As a result of these consequences, nations and information system researchers have engaged in computer crimes of different importance and impact. These offences are analyzed through the exploitation of system vulnerabilities, the distribution of malicious software, the theft of data and funds. This is the origin of the concept "hacker" [6].

International literature and reports are full of information about the security of information systems around the world. One study shows that there are more than 1,500,000 CVEs (Common Vulnerabilities and Exposures) created in the National Vulnerability Database (NVD) since the 1990s until today [7]. In France, a study shows that threats to information systems affect administrations, companies and citizens [8]. The results of this study suggested the improvement of the protection of information systems and data entrusted to the administration, companies and individuals by improving awareness and conducting training on cybercrime.

Therefore, several studies have focused on the variables that influence the security of information systems. By focusing on users' compliance with ICT policies, researchers clarify [9], the notion of cybercrime and place it in a criminological framework where it could be useful for understanding the process of criminalizing new conduct and organizing the organizational and individual response to crime. Through this clarification, they develop technical applications of machine learning for malware detection due to their ability to track the evolution of malware [10]. On the other hand [11], another study analyzed cyber-physical systems widely used in critical infrastructure and presented a methodology to determine the most secure configuration of the cyber-physical system through a public database of cyber vulnerabilities to identify the most secure components of the cyber-physical system. The study also compared cyber risk scores for different cyber-physical system configurations showing that the Windows 10 build 20H2 operating system is more secure than Linux Ubuntu 20.04, while Red Hat Enterprise Linux is the most secure in certain system configurations.

However, in another study [12], experimental results show that threat hunting via adversary emulation has offsetting effects on advanced threat hunting. The results of this study propose the approach of developing the security conscious offensive environment for organizations to discover advanced attack mechanisms and test their ability to detect attacks by adopting simple techniques such as using antivirus software, anti-spyware, operating system update. In this context, it is clear that there is no exact knowledge about the vulnerabilities that threaten computer systems. In order to identify the aspects affecting the security of information systems, this study looks at such an analysis in a public institution of higher education in the Democratic Republic of Congo, specifically at the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College). In doing so, it has been demonstrated that quality education promotes sustainable human development, learning to know, learning to be, learning to live together, learning to do, and learning to transform oneself and society [13].

Through the specialized literature, interesting works are constantly accumulating in the Democratic Republic of Congo. This is the case of a study [14], in which a response is proposed that is based on cyberspace considered as a place without walls in the concrete sense of the term, or even physical dimensions. The study was oriented much more on the legal level than proposing practical computer and cyber security techniques to arm Congolese users of Information and Communication Technologies. However, the rapid development of the Internet has brought convenience and pleasure to life, but with it, many threats and risks have appeared in the network environment [15]. It states that imitation defense is an original integrated defense technology in cyberspace. Although the principle of imitation defense has universal applicability, it still needs to be adapted to the local conditions of different domains. However, it should be noted according to these studies [16] and [17] that Africa is currently experiencing a huge growth of digital technology modifying the behavior of agents in all sectors of activity and this growth has generated a real transformation of society. From these studies [17], shows that the rate of access of the African population to the Internet has recorded an exponential advance as of June 30, 2019, this rate reached 39.8% while it was only 5% in 2007, the world average being 57.3%.

Moreover, [18] shows that Africa, in its multi-faceted environment and whose digitalization is clearly expanding, is trying to gain a foothold without being prepared either in terms of human resources judiciously trained, or on the register of physical and computer infrastructure necessary. So the continent also remains handicapped by the lack of tools and instruments necessary to face the threats and risks generated by the development of cyberspace and its consequences on the national security of its member states.

Furthermore, [18] shows that Africa, in its multi-faceted environment and whose digitalization is clearly expanding, is trying to gain a foothold without being prepared either in terms of well-trained human resources or in terms of the necessary physical and computer infrastructure. So the continent is also handicapped by the lack of tools and instruments necessary to face the threats and risks generated by the development of cyberspace and its consequences on the national security of its member states.

As the daily traffic on the Internet increases dramatically, the digital ecosystem becomes very vulnerable to attacks by digital criminals that endanger the security of users.

Therefore, it is vital for each nation to have an updated legal system capable of effectively protecting users from any criminal behavior typical of this technological environment [19]. Furthermore, [14] states in his study that there has been a significant improvement in telecoms services which today favors the ease of internet connection in the Democratic Republic of Congo. In spite of this evolution, the DRC in turn presents handicaps due to the lack of tools and instruments necessary to face the threats and risks generated by the development of cyberspace and its consequences on national security throughout its territory and in various sectors of activity.

Today, with the proliferation of attack systems and threats that continue to grow, hackers or cyber-attacks change and evolve strategies and methods to attack and threaten Computer Systems. Therefore, it becomes interesting to conduct a study on "The knowledge of cyber security vulnerabilities in an educational institution at the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College)".

The Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) is a public institution of higher and university education, operating in the city of Bukavu, in the province of South Kivu in the Democratic Republic of Congo, which is the population concerned by this study. We have focused this study on an institution of higher and university education because, in the empirical literature, studies of this type have been carried out mostly in Europe, Asia and America and very few in Africa. This is the case of the work of [20], will address the issue of governance of European cybersecurity and in particular to the protection [21] noted that the rapid development of the Internet has brought convenience and pleasure to life, but with it, many threats and risks have emerged in the network environment, so the authors consider that with the presence of the Internet in cyberspace, knowledge about the vulnerabilities that would arise from this development is conceivable and of paramount importance, this is the reason for our study. However, we will focus on the knowledge and mastery of cyber security vulnerabilities in an educational institution at the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) in Congo Kinshasa that has an impact with African realities. In view of the gaps identified in previous studies and in order to cover these gaps, our study proposes to answer the question of how well the agents of the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) have mastered computer vulnerabilities. It is clearly a question of knowing:

- What is the level of knowledge about computer vulnerabilities?
- What is the level of use of anti-virus, Windows update, anti-spyware and firewall software?
- What is the frequency of use of the internet connection by the agents of the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College)?

To answer these questions, our study aims to analyze the level of knowledge of vulnerability and the nature of the computer park of the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College). In other words, this study seeks to verify the level of knowledge of computer vulnerabilities at the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) (1); to analyze the level of mastery and use of security software for computer equipment (2); to detect the frequency of connection to the Internet (3).

2. Concepts Presentations

2.1. Vulnerability

The achievement of these objectives requires the formulation of hypotheses. In response to the research questions posed above, our study assumes that the level of knowledge about computer vulnerabilities at the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) is still critical, the level of use of anti-virus, Windows update, anti-spyware and firewall software is still low, and the frequency of access to the internet by agents at Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) is still high.

After this introduction, our article proceeds with a review of the literature (1), followed by the materials and methods (2) and, finally, the results (3).

Vulnerability as a flaw created during the development of the system, or during its operation, or during its operation [22], which could be exploited to create an intrusion. During the operation of a system, several errors of lack of information can also be added, such as not updating a system, not using software such as antivirus, anti-spyware, firewall, although regularly connected to the Internet. For [23], vulnerability includes measures ranging from semi-formal and formal specification, rigorous design and system management procedures, including user education (e.g., password selection). Vulnerabilities" [24] refers to all weaknesses in computer resources that can be exploited by threats in order to compromise them. Such exploitation can cause significant losses. New vulnerabilities are discovered daily and can affect any IT resource. He detailed three main families of vulnerabilities: Vulnerabilities at the organizational level (Management) which for example study the lack of information of users, vulnerabilities at the physical level the lack of access control to physical elements as for example the access to computer rooms, connectivity or other must be limited to avoid (in)voluntary manipulations, but can cause the global loss of the computer room or connectivity of a part of the users and vulnerabilities at the technological level the case of complexity of rules on firewalls and routers: the implementation of filtering and access rules, on demand, makes it almost impossible to have an overview. The vulnerability scheme according to consists of an autonomous vulnerability assessment approach for individual machines (illustrated in **Figure 1**).

2.2. Life Cycle of a Vulnerability

The life cycle of a vulnerability starts with its discovery (illustrated in **Figure 2**). In case a malicious person discovers it, he will try to exploit it by developing a

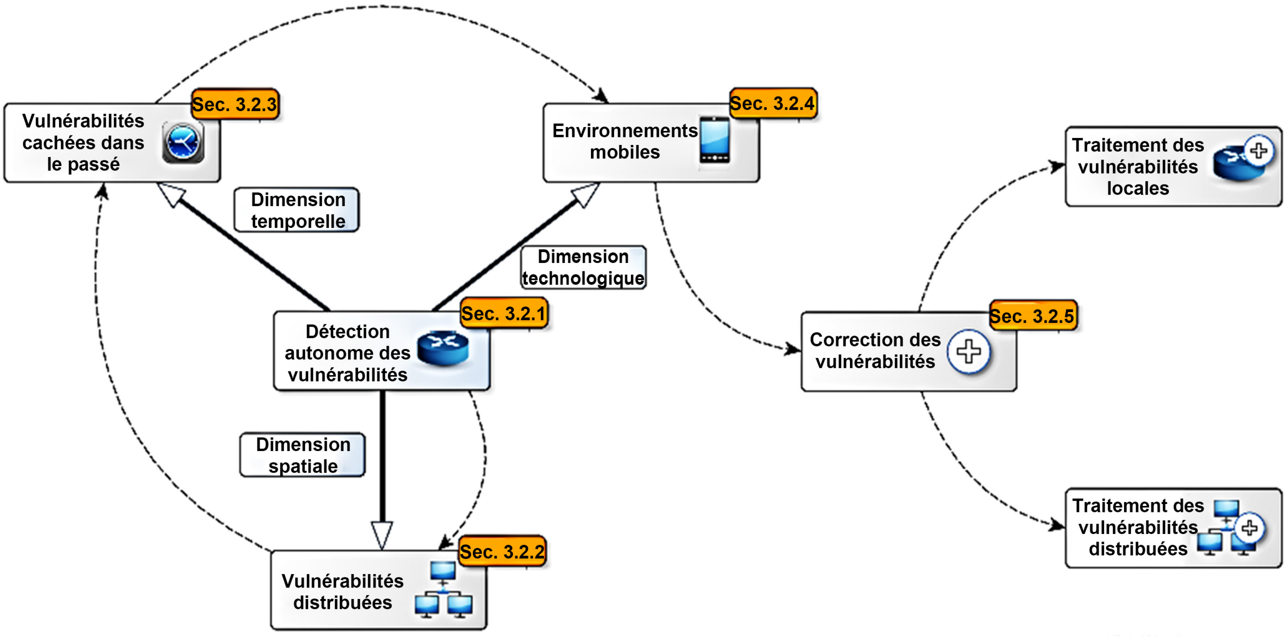
Vulnérabilités cachées dans le passé
Sec. 3.2.3
Environnements mobiles
Sec. 3.2.4
Traitement des vulnérabilités locales
Dimension temporelle
Dimension technologique
Détection autonome des vulnérabilités
Sec. 3.2.1
Correction des vulnérabilités
Sec. 3.2.5
Dimension spatiale
Traitement des vulnérabilités distribuées
Sec. 3.2.2
Vulnérabilités distribuées

Figure 1. Autonomous vulnerability assessment approach by Martin BARRERE CAMBRUN in the summary of his thesis.

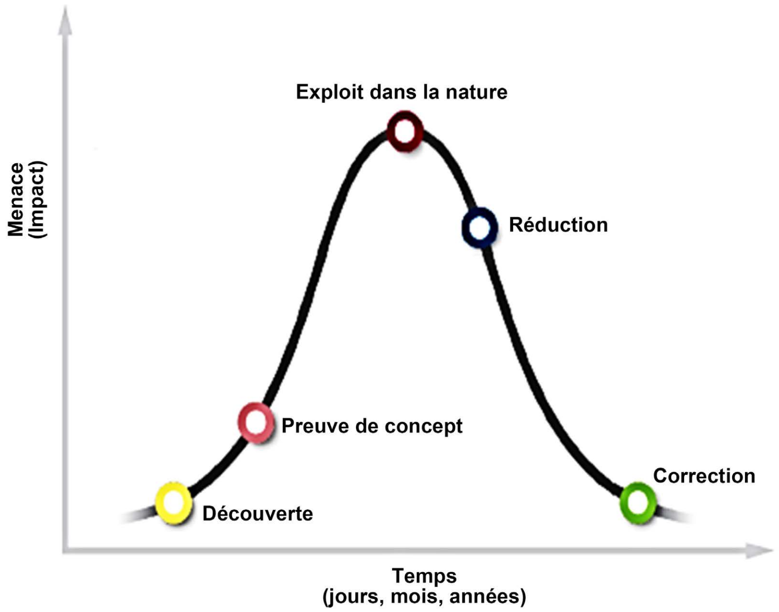

Figure 2. Cycle vulnerability by B. Ere.

specific code called exploit (zero-day) while waiting for this vulnerability to become public, to be qualified and finally to be fixed [3].

The diagram on the right illustrates the life cycle of a vulnerability in terms of the degree of importance of the threat. The organization remains exposed during the entire life cycle, making it necessary to identify the vulnerability as soon as possible and to take it into account quickly.

Causes of Vulnerabilities[1]

Vulnerabilities can be caused by:

- Misconfiguration
- Default installations
- Buffer overflows
- Unpatched flaws on servers
- Operating system vulnerabilities
- Application vulnerabilities
- Default passwords

2.3. Vulnerability Assessment

This is the process of examining the ability of a system or application to withstand attacks. It identifies security flaws in a computer system and communication channels such as open ports, services, misconfigurations, etc., so that improvements can be made.

2.4. Type of Assessment

There are different types of assessment[2]:

[1] https://www2.dijon.inrae.fr/didactepic/Topaze/co/grain_echant-ale-simple.html

[2] https://techno-skills.com/securite/cyber-securite-ethical-hacking/analyse-de-vulnerabilite/

1) Active evaluation: this evaluation acts directly on hosts, services, etc.

2) Passive assessment: this is done by sniffing the network to look for possible vulnerabilities.

3) External assessment: this is an assessment that is done from the outside.

4) Internal evaluation: this is an evaluation from the inside.

5) Host-based evaluation: this type of evaluation is done on a specific host (web server, database server, etc.)

6) Network assessment: this is the direct analysis of the security of a network to identify vulnerabilities.

7) Application assessment: this is the process of assessing the vulnerabilities of an application on a server for example.

8) Wireless network assessment: the assessment is done on the wireless network.

2.5. Computer Risks

There are three factors in determining risk: the nature of the threat, the vulnerability of the system and the size of the asset that could be damaged or rendered unavailable. Risk can therefore be defined as follows:

$$\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Asset}$$

Asset: An asset is sensitive data or what allows access to that data.

Threat: A threat is, for example, a malicious hacker, a criminal or an insider who steals information. A threat can also take the form of an accident, technical failure or user error that may put data (an "asset") at risk.

Vulnerability: A vulnerability is a flaw that can destroy, damage or endanger data.

3. Materials and Methods

In this section, we will present the methodology used to collect the information, the study population and the sample selected, the survey process and the analysis tools.

3.1. The Methodology Used

The data used was collected through a survey conducted among the agents of the ISP Bukavu. The survey was based on the attitudes of the agents of Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) Bukavu towards computer vulnerability. Given the research objectives, we opted for a quantitative approach based on individual interviews. The choice of a methodology is primarily dictated by the research object or problem [25].

3.2. The Selected Sample and the Study Population

The population of this study is made up of 250 employees of Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) Bukavu. As mentioned earlier, we used the quantitative method as a guide. From this population, we drew a simple random sample; a representative sample [26]. We obtained this sample using the following formula [27]:

$$n = N/1 + N(e)$$

From this formula, we obtain a sample of 100 agents with a confidence level of 90% and a margin of error of 6% and a proportion of 60% of the study population. Referring to the study of [28], the questionnaire was given to the respondents, followed by an interview on acceptance of each respondent. The questionnaire concerned the knowledge of computer security vulnerabilities, use of antivirus and anti-spyware software, updating of systems, and the frequency with which agents connect to the Internet. The survey questionnaire consisted of 10 questions. The 100 copies given were correctly answered and were deployed and analyzed. The distribution of the questionnaire was done in the interval of December 2021 until February 2022. The deployment and analysis took place from March to May 2022. The analyses were carried out using the SPSS version 26 software, which facilitated the encoding, the constitution of the database and the descriptive statistics of the variables (illustrated in **Figure 3**).

4. Results

Before presenting the analysis on cyber security, we proceed with descriptive statistics by presenting the socio-demographic characteristics of our respondents. The table above presents the characteristics of the respondents (illustrated in **Table 1**).

4.1. Presentation of The results Obtained

4.1.1. The Gender Agents of ISP-Bukavu

The results of the descriptive statistics show that the majority of ICT (Information and Communication Technologies) users at the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) Bukavu are men. Indeed, 67% of the employees are men and 33% are women (illustrated in **Figure 4**). These results seem to be true insofar as, in most cases, men have a higher access to employment in the university sector than women.

4.1.2. The Age Range of Our Respondents (Illustrated in Figure 5)

Similarly, we can see that the age of respondents varies between 35 - 45 years for the majority. This category represents 41%, while the others represent 23% for the over 50 s, 13% for the 25 - 35 s and 45 - 55 s and 10% for the 18 - 25 s. These results are true because most of our respondents are young and through these

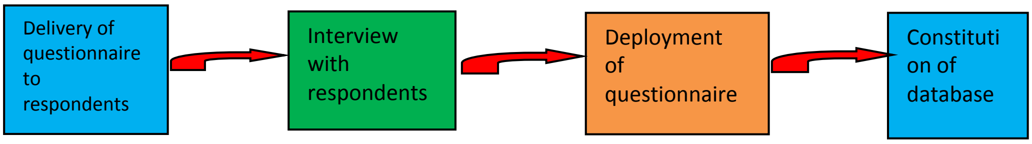
Delivery of questionnaire to respondents
Interview with respondents
Deployment of questionnaire
Constituti on of database

Figure 3. Illustration of the data collection process.

Table 1. Characteristics of the sample.

Characteristics of sample	Frequency	Percentage Participant (N = 250)
Gender		
Male	67	67.0
Female	33	33.0
Age range		
18 - 25 years	10	10.0
25 - 35 years	13	13.0
35 - 45 years	41	41.0
45 - 55 years	13	13.0
55 years and over	23	23.0
Vulnerability		
Yes. I am informed	31	31.0
No. I am not	48	48.0
It is the first time I have heard	21	21.0
Yes. I am informed	31	31.0
Maintenance		
Employees (myself)	16	16.0
IT administrators	58	58.0
External IT person from the institution	26	26.0
Employees (myself)	16	16.0
IT administrators	58	58.0
Windows version		
Windows 11	3	3.0
Windows 10	59	59.0
Windows 8.1	7	7.0
Windows 8	6	6.0
Windows 7	25	25.0
Windows Update		
It is set to update automatically	28	28.0
At least twice a week	3	3.0
At least once a month	3	3.0
Sometimes. when I remember	19	19.0
Never	29	29.0
I don’t know what Windows Upadate is	18	18.0
Antivirus		
Yes	35	35.0
No	47	47.0
Don’t know	18	18.0

Continued

Anti-Spyware		
This is done automatically	33	33.0
At least twice a week	1	1.0
At least once a week	3	3.0
At least once a month	15	15.0
Never	48	48.0
Internet Connection		
Regularly during all service hours	55	55.0
Rarely when dealing with the internet	37	37.0
Never	8	8.0
Firewell		
Yes	15	15
No	50	50
No idea	35	35

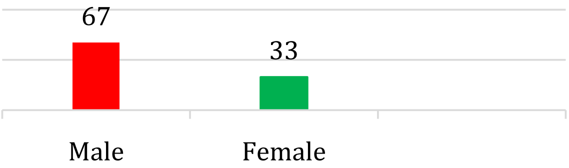

Figure 4. Gender of respondents.

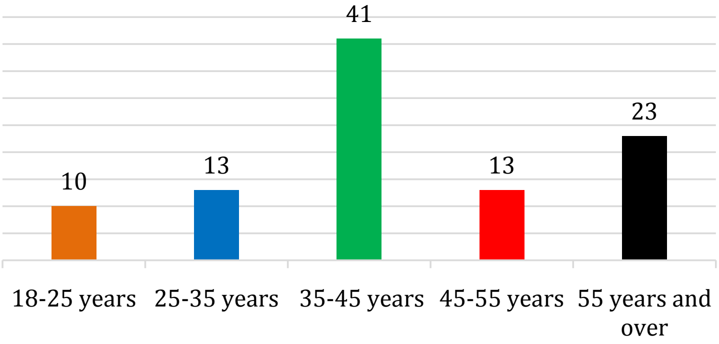

Figure 5. Representation by age group.

results we confirm that it is the youth today who are using ICT (Information and Communication Technologies) in this institution.

4.1.3. Respondents' Knowledge of Computer Vulnerability

With regard to the level of knowledge about computer vulnerability, the level of respondents is as follows: 48% of the sample has no knowledge about computer vulnerabilities, 31% is informed and 21% has no idea (illustrated in Figure 6). These results coincide with the reality at the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) Bukavu. It was noted that the majority

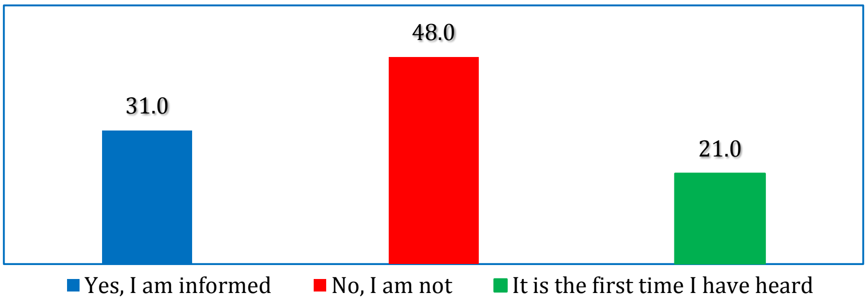

Figure 6. Knowledge about computer vulnerability.

of the agents of this institution remain uninformed about vulnerability due to lack of information, training and popularisation in the face of this scourge. Computer users remain unaware of the dangers of cyber security by working without respecting the basic rules of computer security, which would increase the ease of becoming victims of cyber threats.

4.1.4. Software Installation and Maintenance

Furthermore, it was observed that the majority of software installation and maintenance on office computers is done by computer engineer technician, *i.e.* 58%. Apart from the administrators, 26% of external staff carry out this task. The remaining 16% of our sample is done by the employees themselves (illustrated in Figure 7).

4.1.5. The Version of the Operating System (Illustrated in Figure 8)

Regarding the version of operating system used by respondents, 59% of our sample has installed Windows 10, which in most things that matter such as speed, security, ease of interface, compatibility and software tools, Windows 10 is a considerable improvement over its predecessors. 25% still use Windows 7%, for the Windows 8.1 system, 6%, Windows 8 and 3% Windows 11. 25% still use Windows 7%, for the Windows 8.1 system, 6%, Windows 8 and 3% Windows 11. It appears that the majority of respondents are comfortable with the Windows 10 version. The Windows 10 operating system remains the most widely used today because of its performance and ease of use by users.

4.1.6. Frequency with Which Agents Use Windows Update

With regard to the frequency of use of Windows update, the results show that it varies considerably from one user to another. Users who have never used Windows update 29% of the sample (illustrated in Figure 9). Others on the other hand, the frequency varies from 28% for automatic update, 19% sometimes when they remember, 18% do not know what Windows update is, 3% for once a month and 3% at least twice a week. The results show that this operation is not on the agenda. Indeed, 29% of our sample stated that they never use Windows update due to lack of information and awareness, yet this operation is so important to protect systems against malicious attacks, but also to be on the safe side in terms of security holes discovered in obsolete programs. The operating system

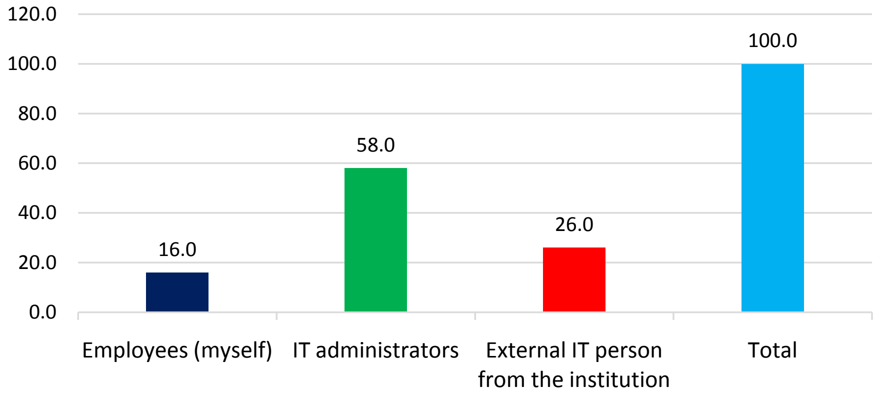

Figure 7. Software installation and maintenance.

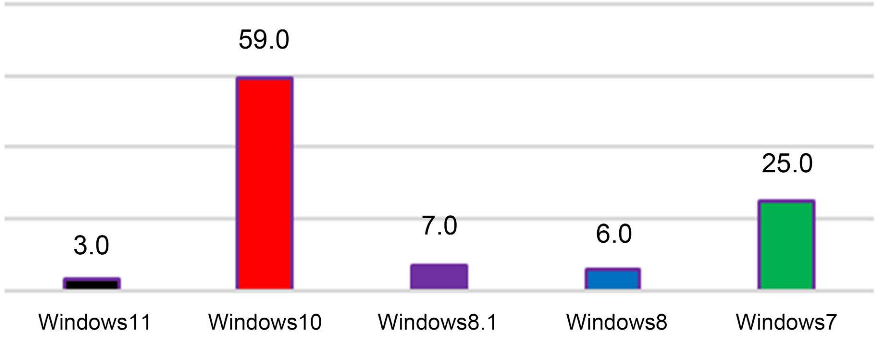

Figure 8. Version of operating system used.

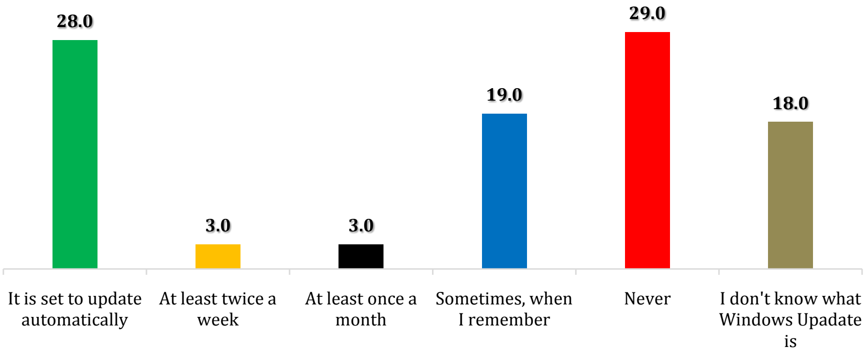

Figure 9. Frequency of use of windows update.

update alone is full of 3 reasons why the latest Windows patches and security updates should be run. These are: Protecting the system from malware, Fixing general Windows problems and bugs and Accessing new Windows and software features. With this 28% increase in frequency for automatic Windows Update essentially allows Windows to do the work for you. This Windows Update feature downloads a security related database to keep the system more up to date with the ever increasing virus vulnerability, will update different types of updates that can increase the security of the system. In this regard, it is highly recommended to keep Windows Update active as well as to update it regularly to avoid vulnerability to various things. Thus, Windows Update will ensure the protection or security of Windows devices.

4.1.7. Installing Antivirus Software on Users' Computers (Illustrated in Figure 10)

After analysis and study, we found that 47% of our respondents do not use or install antivirus software on their computers, although it has several advantages and its main purpose is to detect, neutralise or eradicate malicious software from infected computers and other IT devices. It also plays a preventive role in preventing viruses from infecting and harming computer systems as it will act as a closed door, with a security guard, protecting your system from all kinds of attacks. It protects against several types of malware such as viruses, worms and malware. 35% of our respondents install anti-virus software on their computers against 18% of respondents who do not know anything about anti-virus software, this kind of practice leads to inconveniences such as infection of a computer system with consequences such as: reformatting of the hard disk, loss of data by deleting them, corruption of files, slowing down of the computer, inability of users to work but also spreading of viruses to relatives (illustrated in Figure 10).

4.1.8. The Frequency with Which Anti-Spyware Is Updated

With regard to the frequency with which anti-spyware is updated, 48% of respondents confirm that they never update anti-spyware because they are not informed about security issues at the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) Bukavu. Updating anti-spyware offers the benefits of greater security to users, with the aim of being able to protect a machine against spyware and other malicious software that can be installed on the PC or smartphone at any time without wanting to (illustrated in Figure 11). This type of program helps to reduce the malicious effects caused by spyware, which result in poor computer performance, pop-up windows with warnings, unwanted changes to your PC configuration and unauthorised access to private information. Anti-spyware allows users to protect themselves against software that intends to steal information such as passwords and damage the machine. 33% of respondents confirm that they update automatically to take advantage of all its benefits, 15% at least once a month, 3% at least once a week and 1% at least twice a week.

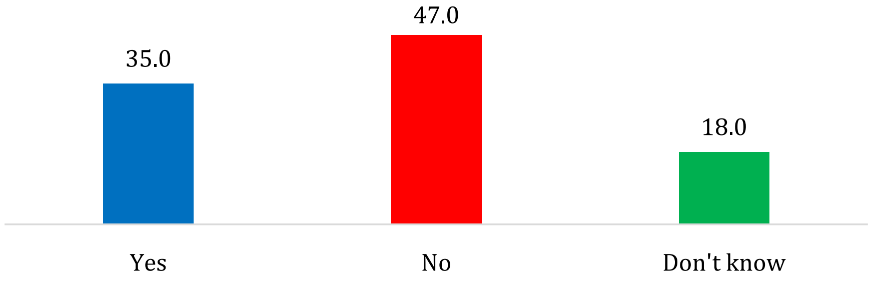

Figure 10. Installation of antivirus software.

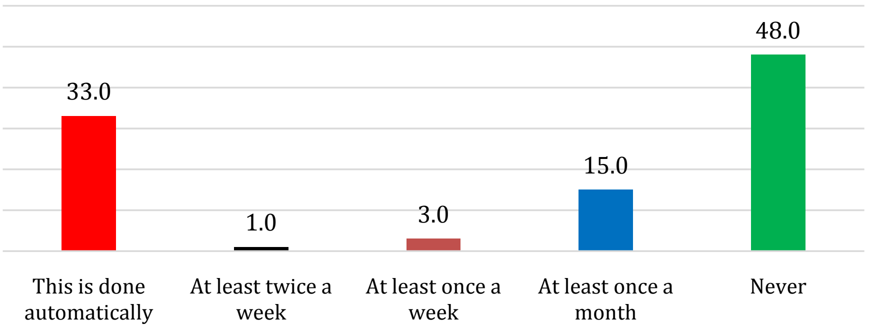

Figure 11. Frequency of anti-spyware updates.

4.1.9. Frequency of Internet Connection by Agents

With regard to the frequency of connection to the Internet, the results show that the frequency is high and important. Agents who regularly connect during all working hours represent 55% of the sample (illustrated in Figure 12). For the other two frequencies, agents with the rare frequency and only logging on when they have something to do on the internet represent about 37% of our sample. Others, on the other hand, never log on (8% of the sample).

4.1.10. The Use of Firewall Software on Agents' Computers

After analyzing the data, it can be seen that respondents do not use firewall software 50% because they are not informed, the same is true for respondents who have no idea 35% and only 15% of respondents confirmed that they use firewall software (illustrated in Figure 13).

4.2. Discussion of the Results and Empirical Verification

Based on our results, we confirm that these results verify the hypotheses assigned at the outset:

By analyzing these results, we note that the majority of users of Information and Communication Technology at the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) Bukavu are men 67% employees and whose majority of age varies between 35 to 45 years and constitutes 41% of our respondents. The choice of cybersecurity is made in accordance with the strategy of the entity and the risks to which it is exposed [29]. Taking note of the technical aspects of informatic security. Regarding the level of knowledge about computer vulnerabilities, the level of respondents is as follows, 48% of the sample has no knowledge about computer vulnerabilities, 31% is informed and 21% has no idea. These results coincide with the reality of the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) Bukavu. It has been noted that the majority of the agents of this institution remain under informed about the vulnerability due to lack of training and popularization in the face of this scourge. Computer users are not aware of the dangers of cybersecurity by working without respecting the basic rules of computer security. Moreover, it was observed that the majority of installations and maintenance of software on office computers is done by computer administrators, that is 58%. Apart from the

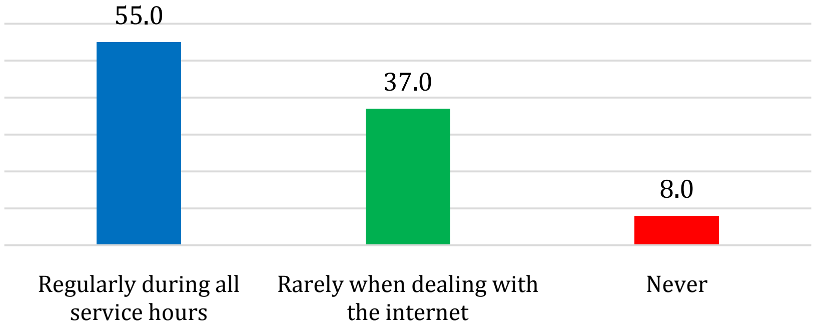

Figure 12. Frequency of internet connection.

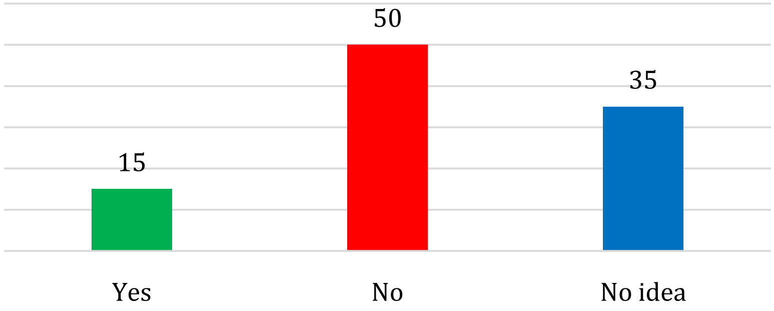

Figure 13. Use of firewall.

administrators, 26% of external personnel perform this task. The remaining 16% of our sample is done by the employees themselves.

Finally, our results showed that the lack of knowledge about computer vulnerabilities which is according to reference [30] an accidental or intentional fault, malicious or not, in the specifications, design or configuration of the system, or in the way it is used, we found that the vulnerabilities are the result of a misuse of the system which is at the root of a low use of computer security measures at the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) Bukavu. These vulnerabilities are therefore timeless and can only be corrected by the users themselves. These results are in agreement with those of [28] who identified: the life cycle of the vulnerability, the behavior of the attacker population and the behavior of the system administrator as the three factors that have an important influence on the state of the system. Thus, the knowledge of vulnerabilities favors the taking of the necessary precautions for the protection of Information Systems through training and awareness. The strategy to fight against cybercrime relies on the sensitization of this study population or the agents of Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) Bukavu. Vulnerabilities are the receptors of threats to which all users of computer systems are subject. Indeed, the exploitation [24] of a vulnerability by a threat can cause significant losses: direct financial losses, loss of reputation and loss of time.

Yet 29% of our sample said they had never used Windows update due to lack of information and awareness and yet this is such an important operation on the use of a computer system to protect systems against malicious attacks, but also to be on the safe side in terms of security holes discovered in outdated programs. The operating system update alone is full of 3 reasons why the latest Windows patches and security updates should be run. These are: Protecting the system from malware, Fixing general Windows problems and bugs and Accessing new Windows and software features. With this 28% increase in frequency for automatic Windows Update essentially allows Windows to do the work for you. This Windows Update feature downloads a security-related database to keep the system more up to date with the ever-growing virus vulnerability, will update different types of updates that can increase system security. In this regard, it is highly recommended to keep Windows Update active as well as to update it regularly to avoid vulnerability to various things. Thus, Windows Update will ensure the protection or security of Windows devices.

To summarize, we say that 48% of the sample has no knowledge about computer vulnerabilities against 31% informed and 21% has no idea; for the use of antivirus software: 47% does not use against 35% who uses and 18% has no idea; for Windows update: 29% never against 28% automatic, 18% no idea, 19% sometimes when he remembers, 3% once a month and 3% other for once a week; for anti spyware: 48% never use against 33% is done automatically, 15% once a month, 3% once a week and 1% twice a week; for the firewall: 50% are not informed against 35% no idea, only 15% informed. This is the consolidation of our study hypotheses.

4.3. Limitations and Future Prospects

Although the results of our study are satisfactory, they are not without limitations. The first methodological limitation of our study concerns the choice of our sample size, which is almost below the average or half of the study population. As the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) Bukavu has 250 staff members, it was difficult to survey all 355 in order to capture the opinions of each individual. In order to do so, we would have had to reach all 250 staff.

Consequently, given the size of the sample, which was smaller than the average for the study population, we could not generalise our results to all staff at the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) Bukavu. Furthermore, the choice of respondents was dictated by the availability of the agents we met to provide us with answers, yet through random sampling, each sample has an equal chance of being selected.

However, these limitations do not diminish the scientific value of this study, as our results remain scientifically valid. Therefore, to address these limitations, we are planning a future study on the identification of cyber security vulnerabilities in a higher education and university institution at the Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) Bukavu by expanding the number of respondents and increasing the equal chance for each sample to be selected, so that this study will be able to propose protection solutions to

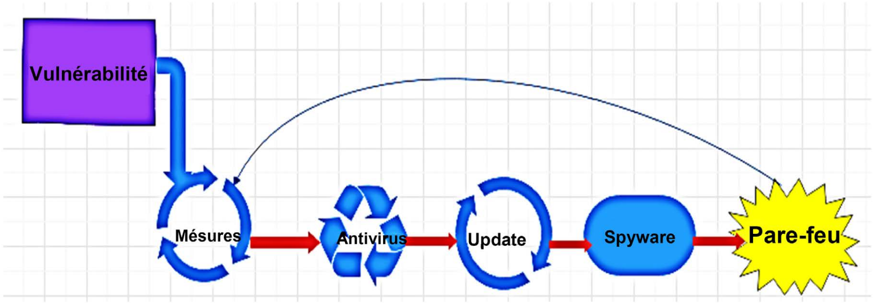

Figure 14. VMAUSP model.

agents. Finally, it will allow us to set up a training platform in the field of cybersecurity.

4.4. State of Play

This part presents the solution, method or model that we have just put in place to help these agents exposed to vulnerability to be able to limit the damage or protect themselves against the threats and vulnerabilities (illustrated in Figure 14). In view of our results, we have proposed a VMAUSP model (Vulnerability, Measures, Antivirus, Update, Spyware and Firewall) represented by the following algorithm

This model shows that after a good knowledge of the vulnerabilities the following measures are taken and implemented: the installation of an antivirus in a computer, the update of the installed operating system, the installation of spyware and the activation of the firewall to put a barrier between the computer and the internet because the results of our investigations proved that these agents most often connect to the internet without considering all these parameters. This was tested by the fact that a training platform on the vulnerabilities of the systems, the measures adopted, the use of licensed antivirus software, the updating of the installed system whenever necessary, the installation of spyware as well as the installation and activation of the firewall for interception between the computer and the Internet is in operation in this institution of higher education and university. According to the study cited in reference [27], when information system policies are not implemented correctly, they become useless documents that make the system more vulnerable, which led us to the creation of this platform for the training of agents of this institution on cyber security matters.

5. Conclusions

Information and communication technologies are experiencing a vertiginous growth almost everywhere in the world, especially in recent years thanks to the development of the Internet. The aim of this study was to verify the level of information of the agents of Institut Supérieur Pédagogique/ISP-Bukavu (TTC = Teachers' training College) Bukavu, users of computer systems, their level of knowledge on the vulnerability to cybersecurity of computer systems in relation to the computer equipment they use, in order to propose a model that would involve the installation of the operating system, maintenance by competent personnel, the frequency of use of anti-virus software, firewall, anti-spyware, updates as well as the frequency with which these agents connect to the internet called VMAUSP (Vulnerability, Measures, Antivirus, Update, Spyware and Firewall). The results showed that the agents are not sufficiently informed about computer vulnerabilities, and the software used to protect themselves is not available, although the frequency of access to the Internet remains high. These results are presented as follows: 48% of the sample has no knowledge of computer vulnerabilities compared to 31% who are informed and 21% who have no idea; for the use of antivirus software: 47% do not use compared to 35% who use and 18% who have no idea; for Windows update: 29% never against 28% automatic, 18% no idea, 19% sometimes when he remembers, 3% once a month and 3% other for once a week; for anti spyware: 48% never use against 33% is done automatically, 15% once a month, 3% once a week and 1% twice a week; for the firewall: 50% are not informed against 35% no idea, only 15% informed. This is the consolidation of our study hypotheses. In order to achieve the expected results, we opted for a qualitative approach based on individual semi-directive interviews, the interview accompanied by a questionnaire. The interview, the direct questionnaire, the observation and the documentary technique served us for the implementation of our research.

However, we do not believe that we have grasped all the contours of this theme, particularly in terms of the methodological choice of our sample size, which is almost below the average or half of the study population. Despite this, it does not diminish the quality of the results obtained. We therefore propose to return to this theme of identifying cyber security vulnerabilities by expanding the number of respondents by increasing the equal chance for each sample to be selected. This will also allow us to integrate other elements and aspects of analysis not taken into account as well as the implementation of a training platform in the field of cyber security.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] L.E.S.D. Techniques (2014) Gestion des vulnérabilités informatiques: Vers une meilleure gestion des risques opérationnels [Valeur et caractère indispensable de la gestion des vulnérabilités].

[2] Karina, D. and Mendoza, O. (2017) The Vulnerability of Cyberspace—The Cyber Crime. *Journal of Forensic Sciences & Criminal Investigation*, **2**, 1-8. https://doi.org/10.19080/JFSCI.2017.02.555576

[3] Ere, B. (2014) Gestion des Vulnérabilités dans les Réseaux et Systémes Autonomes.

[4] Jasmy, M., Rahman, A., Hamzah, M.I., *et al.* (2019) The UKM Students Perception towards Cyber Security. *Creative Education*, **10**, 2850-2858. https://doi.org/10.4236/ce.2019.1012211

[5] Lanotte, A. (2021) Les études qualitatives online: Rétrospective et réflexion sur l'usage ainsi que l'avenir de cette approche dans un contexte de numérisation croissante.

[6] Pawlicka, A. and Pawlicki, M. (2021) The Stray Sheep of Cyberspace a.k.a. the Actors Who Claim They Break the Law for the Greater Good. *Personal and Ubiquitous Computing*, **25**, 843-852. https://doi.org/10.1007/s00779-021-01568-7

[7] Karki, R. and Tsokos, C.P. (2022) Cybersecurity: Identifying the Vulnerability Intensity Function (VIF) and Vulnerability Index Indicator (VII) of a Computer Operating System. *Journal of Information Security*, **13**, 337-362. https://doi.org/10.4236/jis.2022.134019

[8] Stratégie de la France. https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

[9] Leman-Langlois, S. (2015) Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial. *Criminologie*, **39**, 63-81. https://doi.org/10.7202/013126ar

[10] Gibert, D., Mateu, C. and Planes, J. (2020) The Rise of Machine Learning for Detection and Classification of Malware: Research Developments, Trends and Challenges. *Journal of Network and Computer Applications*, **153**, Article ID: 102526. https://doi.org/10.1016/j.jnca.2019.102526

[11] Northern, B., Burks, T., Hatcher, M., Rogers, M. and Ulybyshev, D. (2021) VERCASM-CPS: Vulnerability Analysis and Cyber Risk Assessment for Cyber-Physical Systems. *Information*, **12**, 408. https://doi.org/10.3390/info12100408

[12] Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S.S. and Usman, M. (2020) Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures. *ACM Computing Surveys*, **53**, Article No. 122. https://doi.org/10.1145/3417987

[13] Mahmud, S.N.D. (2017) Systems Structure of Education for Sustainable Development in Higher Education Institution. *Creative Education*, **8**, 1379-1400. https://doi.org/10.4236/ce.2017.89097

[14] Mitongo, P.A.R. and Tr, K. (2010) Notion de Cybercriminalite: Praxis D'une Penalisation Introduction Generale. 1-34.

[15] Chi, X., *et al.* (2020) A Neutralizing Human Antibody Binds to the N-Terminal Domain of the Spike Protein of SARS-CoV-2. *Science*, **369**, 650-655. https://science.sciencemag.org/content/369/6504/650.abstract

[16] Afrique, D. (2020) Congo Lutte contre la cybercriminalité. 1-23.

[17] Mourad, P. and Manir, E. (2019) Le Cyberespace Africain: Un Champ aux Contradictions Manifestes/Africa's Cyberspace: A Field of Clear Contradictions. https://www.africaportal.org/documents/19808/Le_cyberspace_africain.pdf

[18] El Manir, M. (2019) L'afrique face aux defis proteiformes du cyberespace.

[19] Crispin, P., Syosyo, M. and Jel, C. (2014) Analyse du marché des télécommunications mobiles en République Démocratique du Congo: Dynamique du marché et stratégies des acteurs. 1-35.

[20] Bianchi, F. (2017) Impliqués dans la protection des infrastructures d'information critiques. Ouvernance de la cyber-sécurité européenne: Protection des infrastructures d'information critiques.

[21] Miconnet, E., Bettan, O., Gidoin, D. and Jouenne, E. (2013) Un exemple d'usage des graphes d'attaques pour l'évaluation dynamique des risques en cyber-sécurité des

graphes d'attaques.

[22] Welch, I., Warne, J., Ryan, P., Stroud, R., *et al*. (2003) Architectural Analysis of MAFTIA's Intrusion Tolerance Capabilities. School of Computing Science Technical Report Series.

[23] Reddy, A.V., Sharath Kumar, K. and Prasad, V.H. (2013) Intrusion Detection on Cloud Applications. *International Journal of Computer Science and Mobile Computing*, **2**, 1-7. https://www.ijcsmc.com

[24] N. Technologies. Vulnérabilités. https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/Vulnerabilites.pdf

[25] Allnutt, V. (2012) Étude qualitative sur les attitudes des bibliothécaires québécois vis-à-vis la liberté intellectuelle et la censure.

[26] P. L. E. S. Organisations (2016) Méthodologie de la recherche scientifique.

[27] Kothari, C.R. (2004) Research Methodology. *Methods and Techniques*, **4**, No. 1.

[28] Semlambo, A.A., Mfoi, D.M. and Sangula, Y. (2022) Information Systems Security Threats and Vulnerabilities: A Case of the Institute of Accountancy Arusha (IAA). *Journal of Computing and Communication*, **10**, 29-43. https://doi.org/10.4236/jcc.2022.1011003

[29] Alsulami, H., Khayyat, M., Aboulola, O.I. and Alsaqer, M.S. (2021) Development of an Approach to Evaluate Website Effectiveness. *Sustainability*, **13**, 1-15. https://doi.org/10.3390/su132313304

[30] Gaye, A. (2020) Etude des vulnérabilités informatiques liées à la pandémie du coronavirus.

Sites Links

https://www2.dijon.inrae.fr/didactepic/Topaze/co/grain_echant-ale-simple.html

https://techno-skills.com/securite/cyber-securite-ethical-hacking/analyse-de-vulnerabilite/