Cybercrime in Morocco

A Study of the Behaviors of Moroccan Young People Face to the Digital Crime

M. EL Hamzaoui[1]
Laboratory of Innovation in Science, Technologies and Modeling (ISTEM)
Faculty of science, University Chouaib Doukkali
El Jadida, Morocco

Faycal Bensalah[2]
Lab STIC
Faculty of science, University Chouaib Doukkali
El Jadida, Morocco

***Abstract*—Cybercrime encompasses all illegal actions and facts that target cyberspaces and cause enormous economic and financial damages to organizations and individuals. A cyberspace is essentially composed of digital information as well as its store and communication instruments/platforms. To remedy this phenomenon, attention has focused particularly on both computer security and legislation in an area where the human behavior is also decisive. Social psychology has well defined the concept of behavior and also studied its relations with the attitude in human action. This paper aims to broaden the scope of cybercrime to also discuss marginal phenomena which do not attract enough attention but could easily be converted to digital criminals once circumstances become appropriate. The main objective of this work is the study of the 'human'-'digital world' interactivity in a specific geographical area or precisely the study of the human behavior towards digital crimes. The proposed study targets young people of a small Moroccan city that is in the south of the country central region and constitutes its global economy barycenter. The study dealt specifically with a sample of Moroccan young living in El Jadida city that coincidentally contains individuals from other Moroccan cities which enriched this study more.**

***Keywords*—Cybercrime; cyberspace; information system; information and communication technologies; social psychology**

I INTRODUCTION

Cybercrime is a synonym for digital crime. However, this simplified definition cannot hide the phenomenon dark side; cybercrime is characterized by a variety of dangers able to cause enormous financial and economic damage [1,2].

Cybercrime does not have a definition that specifies its general framework and its dimensions. Since cybercrime is strongly linked to cyberspaces, its definitions [3,4] converge almost completely on this common idea: "Cybercrime is, generally, a phenomenon able to target illegally computer-assisted activities opened on communications' networks". In general, cyberspaces are the technologies and platforms used for the storage and communication of digital information.

Practically, organizations (enterprises, administrations, etc.), that adopt a good governance in the management of their digital environments use, on the one hand, Information Systems (IS) to manage, store and manipulate digital information and, on the other hand, Information and Communication Technologies (ICT) to communicate it.

Historically, cybercrime dates back to the 1980s and 1990s. In 1988, Robert Morris released a program onto Internet (worm [5]) to find out how many computers were currently connected to it but a bug in this program caused damage to many computers in US. Legislatively, this act is classified as one of the Digital World (DW) first crimes.

The fight against this phenomenon attracted especially the interest of computer scientists, lawyers and academics [6,7,8,9]. Therefore, computer security and legislation became the main tools to fight against cybercrime but other interesting parameters are still neglected. For example, given its effects on human uses of DW services [10], the parameter of human behavior will be very useful in the fight against cybercrime.

The specialists of people security and installation safety use the "human factor" concept to refer to the men behavior inside work environments [11]. In general, the human factor refers to the contribution of the human being to events and is also involved in the study of relationships between human behavior and environments, in which man can act on actions, undergo effects or make changes.

In this context, the social psychology studies relationships links attitude to behavior in human action and develops theories and models to facilitate the comprehension of the enigmas of human attitude, behavior and action in society. Along with this work, we will respect and adopt the social psychology terminology as well as the scientific perception of behavior defined and used in some research works of this field.

This paper also draws attention to a new issue concerning certain phenomena that could be converted into digital crimes when circumstances permit. Therefore, we have, on the one hand, to re-draw the cyberspace dimensions to include all data that could be used indirectly in digital crime and, on the other hand, to generalize the cybercrime definition in order to consider these dangerous phenomena: "*Cybercrime is a multidimensional phenomenon (legislation, technical, social, societal, etc.) able to target randomly (directly and/or indirectly and at any time), through all illegal means (hacking, destruction, theft, corruption, etc.), cyberspaces composed mainly of information, IS, ICT and any other instrument, platform or electronic/non-electronic device used to store or to communicate information.*"

This work aims to present, through a study on the El Jadida young people behaviors in the face of digital crimes, the role

that the human behavior could play in the fight against cybercrime.

II Theoretical Framework

A. Fight against Cybercrime between Computer Security and Legislation

The preferred preys of DW criminals are cyberspaces including digital information (mobile and immobile). Digital dangers are all actions that can randomly target digitalized parts of any personal or organizational activity and cause massive damage (e-commerce [12], logistics [13], finance [14,15], marketing [16,17], etc.).

The fight against cybercrime is therefore a complex and multidimensional operation that mainly involves computer security specialists and lawyers:

Concerning the computer security, The OSI 7498-2, second part of the reference model for open systems interconnection (OSI 7498 model), specifies the security architecture through a detailed description of the computer networks security. The computer networks security management is a main functional area of the OSI management [18] that covers the basic digital security objectives (Preventing unauthorized divulgations of data, prohibition of unauthorized modifications of data, prevent unauthorized access to resources, etc.). The digital environments can also be secured in different manner such as electronic certificates, authentication and authorization, Secured communication channels (VPNs), and DMZs.

Concerning the legislation relating to cybercrime, several works were dealing this subject [19,20] but obstacles and constraints were being and are still numerous and complex [21]. Then, the global success of the fight against cybercrime requires the harmonization of legislative efforts undertaken in geographical areas characterized by their territorial sovereignties (countries, unions, etc.) but differ in legislative, cultural and other specificities.

In this context, the most active UN-institution in reaching harmonization on global cybersecurity and cybercrime legislation is the International Telecommunication Union (ITU) in Geneva [20] that has developed a guide to help developing countries understand the legal aspects of cybercrime and to contribute to the harmonization of legal frameworks.

According to Schojolberg [20], the long history of global harmonization on cybercrime legislation was initiated by Donn B. Parker research of computer crime and security from the early 1970ties and it could then evolve through various scientific works and manifestations.

In Morocco, our study geographical zone, since the begin of the 21th century, enormous efforts have been made in this regard (new laws were promulgated, proposition of numeric projects as the “Maroc Numeric 2013” strategy, ratification of the Budapest Convention of 23 November 2001 on cybercrime, etc.).

B. Overview on the Behavior in Social Psychology

This work is intertwined with social psychology, which focuses on relationships that can link attitude to behavior in human action. In this field, several theories and models have been proposed to understand and illustrate the main concepts such as human attitude, behavior and action in society:

The Theory of Reasoned Action (TRA) [22] was developed by Fishbein and Ajzen (1967) to predict how individuals behave according to their pre-existing attitudes and behavioral intentions. Then, in 1985, Ajzen developed 'Theory of Planned Behavior' (TPB) [23], an improved version of the TRA, by adding to its behavioral control. The TPB was developed to predict and explain human social behavior, and to serve as a framework for behavior change interventions.

In Ajizen's research works, behavior is defined as the manifest, observable response in a given situation with respect to a given target and immediately preceded by the intention that expresses the person's readiness to perform a given behavior. According to the TPB, the intention itself is based, on three basis factors; namely the ‘attitude toward a behavior’ that allows to know the degree to which performance of the behavior is positively or negatively valued, the ‘Subjective norm’ that encompasses the perceived social pressure to engage or not in a behavior and the ‘Perceived behavioral control’ that refers to people's perceptions of their ability to perform a given behavior (Fig. 1). Moreover, the ‘behavioral control’ is a main key of the success of a behavior performance.

In short, the TPB states that human behavior is channeled through three mains axes which are behavioral beliefs, normative beliefs and control beliefs.

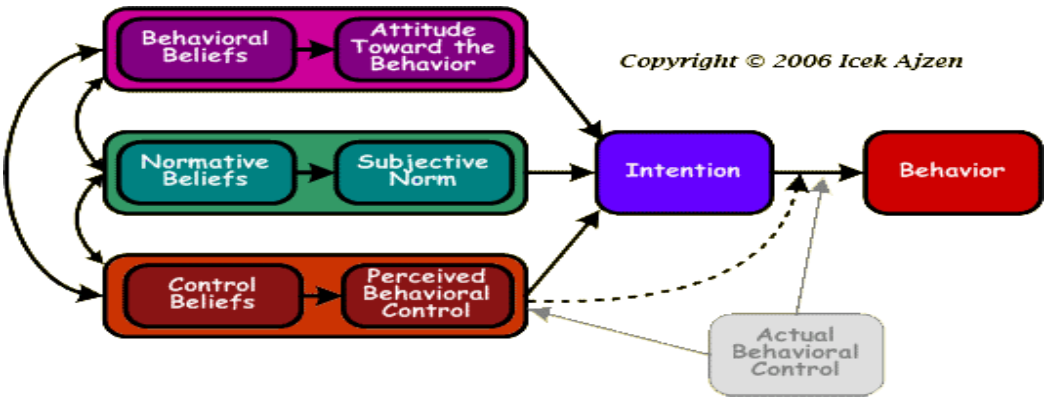


Fig. 1. Schematic Representation of the ‘Theory of Planned Behavior’.

III Convertible Phenomena to Digital Crimes

Cybercrime is the set of classic digital abuses (hacking, interception, destruction, etc.) as well as other digital crimes that could be grow in proportion to the development of digital services on Internet (Frauds with blue card, digital identity theft, etc.).

Unfortunately, the fight against cybercrime had focused on the digital aspect of information and neglected phenomena that are able to touch, with or without bad faith, any type of information (written texts, discussions, etc.) in order to digitize and to use them in digital crimes. Henceforth, these phenomena will be called, along this paper, the Convertible Phenomena to Cybercrimes (CPC).

The CPC constitute a result of both very particular actions and individual or collective behaviors, voluntary or not, which especially related to the individual and/or managerial imprudence within organizations but also in private area (trust to the other, lack of belonging workplace spirit, security vulnerabilities, etc.). The CPC do not attract enough attention from the responsible of their living environments and are also characterized by important properties make them dangerous such as the ability of randomly conversion into digital crimes, the dependence on geographical specificities (traditions of workspaces, social customs, etc.), etc.

For example, in North Africa cities, one can sometimes find easily, in the peanut vendors' shop, personal and organizations archives documents containing extremely sensitive data (financial transactions, commercial actions, etc.). These information leaks can cause damage to organizations and lead to serious social crises for individuals.

Similarly, according the some countries' traditions, the discussions between organization' employees, in public places (cafes, public transport, etc.), could facilitate the disclosure of secrets which are well hidden and clasped in the organization vaults. These verbal data could be digitized (digital texts, voice recordings, etc.) and then misused in the DW. Despite the lack of statistics and studies on the CPCs, they are certainly involved in digital crimes.

Concerning the based bad faith CPCs (aggression, scam, corruption, etc.), we can cite the example of the criminals who illegally remove, in the real world, sensitive digital information (information of a bank account, electronic device password, etc.) for illegal uses in the DW.

IV Realized Study: Young Moroccan People and Cybercrime

A. General Framework of the Study

In Morocco, as in any other country, it is difficult to limit to technology and legislation in the fight against cybercrime. In this perspective, to facilitate the discovery of the possible relations between human behavior and digital crime, we conducted a quantitative study on a random, representative and varied sample of young people from a carefully selected Moroccan city.

TABLE I. Different Axis of our Quantitative Study and their Objectives

Axis	Objective
1	Collection of respondents' personal data.
2	Measure of the degree of the respondents' familiarization with the digital world.
3	Measure of the vigilance of the respondents in the digital world.
4	Knowledge of the respondents' judgments on computer security.
5	Discovery of the respondents' behaviors towards crimes opportunities.
6	Discovery of the respondents' opinions on both cybercrime in Morocco and its relative legislation.

This quantitative study dealt with six fundamental axes where each one is distinguished by a set of criteria defining its own nature (Table I). The axes' objectives are will arranged in order to facilitate the realization of the entire study objective; the study of human behavior in the face of digital crime.

Moreover, the study axes will allow us to define the respondents' personalities and the necessary components to determine their behaviors in accordance with the social psychology principles. Then, theses axes will allow us to know the various factors determining the respondent's intention to choose and adopt a new behavior:

- The degree of the respondent's acceptance of both his future behavior and the potential consequences.
- The influence of the environment on the respondent behavior.
- The beliefs about the respondent's ability to succeed in his future adopted behavior.

B. The Study Results: Data and Statistics

The main data collected in our quantitative study are presented in Tables II, III, IV, V and VI.

Concerning the last criterion of the third axis (Table IV), a rate of 39.53% of the respondents who were never victims of the DW know victims of this world.

C. Synthesis of Obtained Data

Because of quantitative studies aims to give approximate results close to the observed reality, we have chosen to work in the following syntheses on intervals instead of exact values that vary from a study to another. This approach will allow us to define, for each synthesis case, a Logic Interval of its Study and Realization (LISR); an interval where it could really take place.

To facilitate the synthesis of the obtained results, we proceeded to a new repartition of the study six axes in four homogeneous and coherent synthesis operations.

1) Synthesis 1: Personal data

We note a strong coherence between age and study level criteria (Table VI) for all respondents. Only 4% of the respondents, aged between 6 and 12, are college students while just 1% of them, aged between 16 and 18, are university students. Then, the respondents are characterized by a certain study level advancement with respect to age, which proves the quality of the studied sample.

TABLE II. RESULTS OF THE CRITERIA OF THE FIRST AXIS OF OUR QUANTITATIVE STUDY

Axis	Criterion	Obtained Result
1	Age	- *Between 6 and 12 years:* 10% of the respondents global number. - *Between 13 and 15 years:* 26% of the respondents global number. - *Between 16 and 18 years:* 33% of the respondents global number. - *Plus, then 18 years:* 31% of the respondents' global number.
	Study level	32% of the respondents are university students, 32% are high school students, 30% are middle school students and 6% are primary school students.
	Origin city	Majority of the respondents come from El Jadida (55%) followed by Casablanca (31%). Other origin cities (Rabat, Fez, Safi, Settat, Khouribga, Marrakech, etc.) together represent a rate of 14%.

TABLE III. RESULTS OF THE FIRST CRITERION OF THE SECOND AXIS OF OUR QUANTITATIVE STUDY

Axis	Criterion	Obtained Result				
		Very high	***Rather high***	***Medium***	***Rather weak***	***Very low***
2	Degree of familiarization with Internet	31%	24%	31%	4%	10%

TABLE IV. RESULTS OF THE CRITERIA OF THE AXES 2,3,4 AND 5 OF OUR QUANTITATIVE STUDY

Axis	Criterion	Obtained Result	
		Yes	**No**
2	Being used to purchase on Internet	51.00%	49.00%
3	Knowledge of risks related to purchase on Internet	58.60%	41.40%
	Being, one day, a victim of the digital world crimes	14.00%	86.00%
	Knowledge of the digital world victims	37.80%	62.20%
4	Effectiveness of computer security tools in the fight against the digital world risks	54.00%	46.00%
	Possibilities of digital attacks in the absence of computer security tools	67.00%	33.00%
5	Being aware of the risks involved in committing a crime	50.00%	50.00%
	Audacity to commit crimes in the face of an excellent opportunity in the real world	11.00%	89.00%
	Audacity to commit crimes in the face of an exceptional opportunity in the digital world	30.00%	70.00%

TABLE V. RESULTS OF THE CRITERIA OF THE SIXTH AXIS OF OUR QUANTITATIVE STUDY

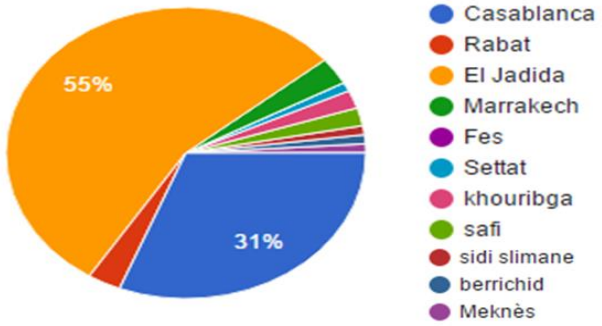
Axis	Criterion	Obtained Result				
		Relevant	***Fairly relevant***	***Medium***	***Fair weak***	***Very weak***
6	Judgment of the relevance of the Moroccan legislation on cybercrime	11%	12%	33%	17%	11%
	Evaluations of the cybercrime in Morocco	mediocre, a phenomenon with unclear legislation and threatens the DW, an evolving phenomenon against a rigid legislation, etc.				

TABLE VI. COHERENCE BETWEEN AGE AND STUDY LEVEL OF THE RESPONDENTS SAMPLE

	Interval	Percentage		Percentage	Level	
Age (years)	≥ 19	31%	←→	32%	Ens. Sup	**Study level**
	[16,18]	33%	←→	32%	High School	
	[13,15]	26%	←→	30%	College	
	[06,12]	10%	←→	6%	Primary School	

Basing on these data, we can define two major blocks; namely the Block of the University and High School Students (BUHSS) and the Block of the Middle and Primary Schools Students (BMPSS).

(a). Map Positions of Some Origin Cities of the Studied Sample.



(b). Repartition of the Origin Cities of the Studied Sample.

Fig. 2. Geographical Positions and Repartition of Origin Cities of the Study Respondents.

The Number of the BUHSS (NBUHSS) represents 64% of the Total Number of the Studied Population (TNSSP) while the Number of the BMPSS (NBMPSS) represents a percentage of 36%.

Considering the study role in the determination of the human behavior, we will analysis the criteria of our study axes according to the "Study Level" criterion, especially according to BUHSS and BMPSS.

In this study, the main reason to consider the city criterion (Fig. 2) is that the city is a geographical area where cultural exchange profoundly influences individual behavior.

The chosen sample survey covers almost all main cities of the Moroccan large central region and also extends to reach a few cities on its borders (Fig. 2(a)). This diversity of the origin cities characterizing our studied sample (Fig. 2(b)) will certainly increase our knowledge level about young people in many Moroccan cities where regional cultures intervene strongly. Therefore, this will allow us to easily generalize the study results on all Moroccan young.

2) Synthesis 2: Interactivity with the DW

- *Use of Internet network services*: A rate of 86% of the respondents is considered familiar with Internet but 14% of them are not (Table III).

The study of this criterion according to the study level criterion gave us:

Relatively to the TNSSP, if V% ($0 \leq V \leq 14$) is the percentage of the BUHSS respondents '*Non-Familiarized with the Utilization of the Internet Services, NFUIS*', the NFUIS percentages relative to the NBUHSS and the SBMPSS are respectively:

- *P1: Number (NFUIS of BUHSS)/NBUHSS = V/64*
- *P2: Number (NFUIS of BMPSS)/NBMPSS = (14-V)/36*

In principle, the unfamiliarity with the DW decreases with the increase of the study level, which implies that the percentage of the NFUIS inside the BUHSS relative to the NBUHSS must be lower than the percentage of the NFUIS inside the BMPSS relative to NBMPSS.

Therefore, one can define, in Fig. 3, two zones on both sides of the point V=8.96 (P1=P2=14%) and deduce that the closest situation to reality must be in the second zone (V<8.96) (Table VII); when the variable X tends to zero.

- *Purchase on Internet*: A percentage of 51% of the TNSSP make purchases on Internet (Table IV) which represents 59.30% of all the respondents familiar with the DW. In reality, only those familiar with the DW can purchase on the Internet. This situation may be due to the lack of online purchasing services (technical and technological constraints), lack of digital trust, etc.
- *Consequences of the Internet services uses*: A percentage of 58.6% of the TNSSP knows risks related to the purchase on Internet but 41.40% of them ignore these risks (Table IV).

Relatively to the TNSSP, if W% ($5.4 \leq W \leq 41.40$) is the percentage of the respondents '*Ignorant of the Internet Purchased Risks, IIPR*', the IIPR percentages relative to the NBUHSS and the NBMPSS are respectively:

- P1: Number (IIPR of BUHSS)/ NBUHSS = W/64
- P2: Number (IIPR of BMPSS)/ NBMPSS = (41.40-W)/36

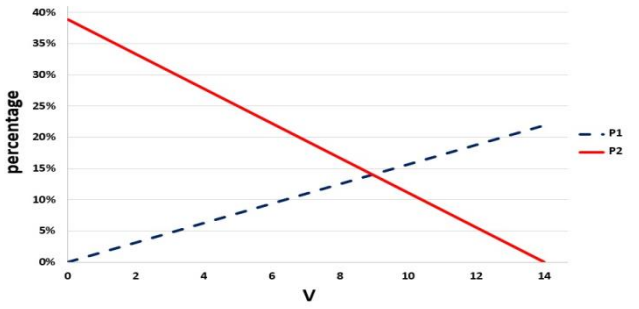


Fig. 3. Percentages of the NFUIS Relative to the BUHSS and the BMPSS.

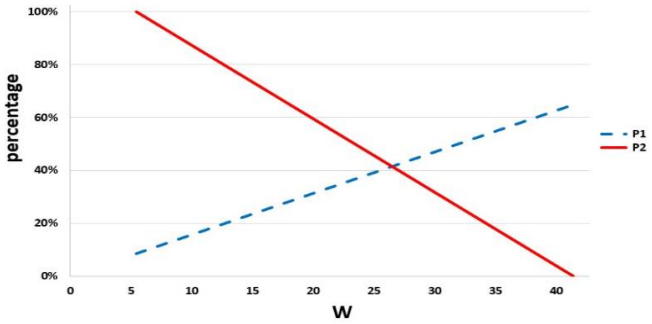


Fig. 4. Percentages of the IIPR Relative to the BUHSS and the BMPSS.

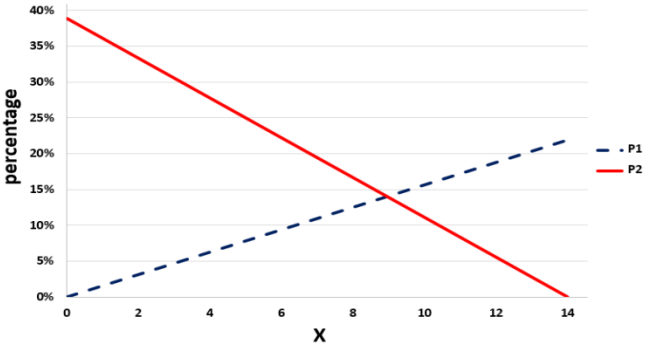


Fig. 5. Percentages of VDWC the Relative to the BUHSS and the BMPSS.

TABLE VII. LISR AND EXTREME CASES OF THE VARIABLE V

Zone	Extreme Cases	LISR
V>8.96	V=14, P1=21.88%, P2=0%	
V<8.96	V=0, P1=0%, P2=38.39%	[0,8.96]

TABLE VIII. LISR AND EXTREME CASES OF THE VARIABLE W

Zone	Extreme Cases	LISR
W>26.50	W=41.40, P1=64.69%, P2=0%	
W<26.50	W=5.5, P1=8.44%, P2=100%	[0,26.5]

TABLE IX. LISR AND EXTREME CASES OF THE VARIABLE X.

Zone	Extreme cases	LISR
X>8.96	X=14, P1=21.88%, P2=0%	[8.96,21.88]
X<8.96	X=0, P1=0%, P2=38.89%	[0,8.96]

In principle, the knowledge of the risks of purchases on the Internet depends on the level of study and also increases relative to it. Therefore, one can define, on Fig. 4, a study area on each side of the point W=26.50 (P1=P2=41.40%) (Table VIII) and conclude that the interval [0,26.5] may be the LISR of this criterion since the IIPR percentage relative to the middle and high schools students total number exceeds that of the BUHSS.

In this context, the DW risks most known by the respondents are principally scam, late delivery, counterfeiting and piracy.

- Being a victim of the DW crimes: Only 14% of all respondents were victims of the DW and 86% of them are not (Table IV).

Relatively to the TNSSP, if X% ($0 \leq X \leq 14$) is the percentage of the respondents of the BUHSS '*Victims of the DW Crimes, VDWC*', the percentages of the VDWC relative to the NBUHSS and the NBMPSS are respectively:

- P1: Number (VDWC of BUHSS)/NBUHSS = X/64
- P2: Number (VDWC of BMPSS)/NBMPSS = (14-X)/36

Before interpreting the data and treating these two equalities, we recall that all data on VDWC and NFUIS, including percentages, coincide perfectly. Therefore, the variables X and V behave in the same way, which increases the probability that the NMMV inside the studied sample can be exactly its NFUIS.

The discussion of the extreme cases of this criterion, as illustrated in Fig. 5, led to the definition of two zones on both sides of the point X=8.96 (P1=P2=14%) (Table IX).

On the one hand, if the NBMPSS uses the digital services more correctly than the NBUHSS, the first Zone (X>8.96) may be a LISR of this criterion. In this case, between 14% and 21.88% of the university and high school students of EL Jadida city could be DW victims.

On the other hand, the second Zone (X<8.96) represents an LISR of this criterion if the NBUHSS uses correctly the DW services. In this case, between 24.89% and 38.89% of the primary and middle school students of El Jadida city could be DW victims.

Moreover, we recall that 37.8% of the TNSSP know VDWC but 62.2% of them do not know anyone. In addition, a percentage of 39.53% of the respondents who were never the VDWC know VDWC, but only 3.81% of those who were the VDWC know VDWC. Therefore, it is clear that the knowledge of VDWC increases the level of vigilance in the use of the digital services.

- Effectiveness of Computer Security Tools in the Fight Against Cybercrimes (CSTFAC): The interval of the percentage of NBUHSS individuals who do not trust the effectiveness of the CSTFAC is [15.64%, 71.88%] while that relative to the BMPSS is [0%,100%]. Consequently, at least 28.31% of the BUHSS trust the CSTFACs but this percentage will never exceed 84.36%.

The percentage of individuals, who believe that machines could be in safe without computer security tools, is 33%, which is a weak percentage. If one considers that only the VDWC who underestimate the computer security importance, one can then deduce that 42.42% of these individuals are the VDWC.

3) Synthesis 3: Behaviors of the Respondents in the Face of the Crimes Opportunities

Firstly, we remember that the half of the TNSSP (50%) is aware of the dangers of committing any kind of crimes.

- *Behavior in the face of the opportunities for safe crime:* A percentage of 11% of the TNSSP has the audacity to perpetrate crimes in the real world if conditions are favorable while 89% of them cannot do.

Because of, as it is already mentioned, the CPC can take place, with or without bad faith, we can conclude that, in this case, 11% of the TNSSP could voluntarily support the CPC while 89% of them could do it accidentally. Concerning the digital crime, a percentage of 30% of the TNSSP has the audacity to perpetrate this kind of crimes while 70% of them do not have it. One notes that the rate of people with the audacity to commit crimes increases by 272.73% from the real world to the DW.

Relatively to the TNSSP, if Y% ($0 \leq Y \leq 30$) is the percentage of the BUHSS respondents '*Able to Perpetuate Digital Crime, APDC*', the percentages of the APDC relative to the NBUHSS and to the NBMPSS are respectively:

- P1: Number (APDC of BUHSS)/NBUHSS = Y/64.
- P2: Number (APDC of BMPSS)/NBMPSS = (30-Y)/36.

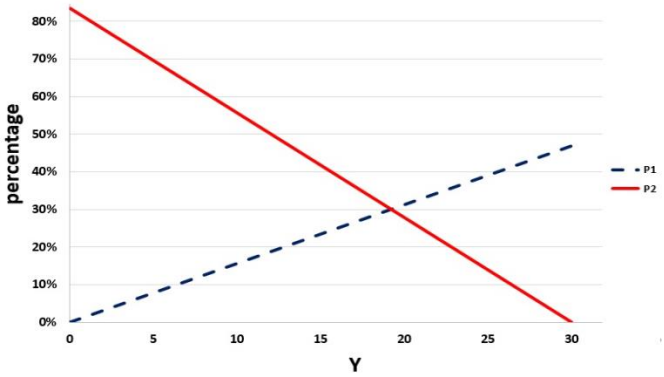


Fig. 6. Percentages of the APDC Relative to the BUHSS and the BMPSS.

TABLE X. LISR AND EXTREME CASES OF THE VARIABLE Y

Zone	Extreme cases	LISR
Y>19.20	Y=30, P1=46.88%, P2=0%	[19.20,30]
Y<19.20	Y=0, P1=0%, P2=83.33%	[0,19.20]

The consideration of the study level allows to define, on Fig. 6, two zones on both sides of the point Y=19.20 (P1=P2=0%) (Table X):

The Zone (Y>19.20) could be a LISR of this criterion when, on the one hand, the NBUHSS is well familiarized with the DW but without responsibility and, on the other hand, the NBMPSS is well surrounded and well supervised. We warn that, depending on the circumstances and the entourage, up to 46.88% of the NBMPSS could become digital thieves.

The Zone (Y<19.20) could be a LISR of this criterion when the individuals of the BMPSS are clumsy in the WD but those of the NBUHSS are correct. We warn that up to 83.33% of the SBMPSS could commit crimes in the DW. A dangerous social phenomenon could take place if the parents, education system and responsible will not intervene to anticipate, sensitize and supervise these young people.

4) Synthesis 4: Cybercrime in Morocco

- *Moroccan legislation on cybercrime:* A percentage of 72% of the TNSSP judges positively this legislation while 28% of them judge it negative (Table V).

Relatively to the TNSSP, if Z% (36≤Z≤64) is the percentage of the BUHSS respondents having '*Positive Judgments to the Moroccan Legislation Relating to Cybercrime, PJMLRC*', the percentages of the PJMLRC relative to the NBUHSS and the NBMPSS are respectively:

- P1: Number (PJMLRC of BUHSS)/NBUHSS = Z/64
- P2: Number (PJMLRC of BMPSS)/NBMPSS = (72-Z)/36

The study level is very important in the interpretation of this criterion because in principle the NBUHSS are well placed than the NBMPSS to judge adequately specific legislations.

As for previous cases, one can defines, as illustrated on Fig. 7, a study area on each side of the line joining the points P1=P2 (=72%) and the point Z=46.08 and also specifies the criterion LISR (Table XI).

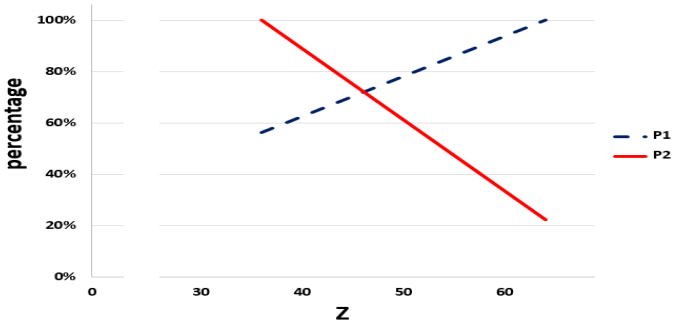


Fig. 7. Percentages of the PJMLRC Relative to the BUHSS and the BMPSS.

TABLE XI. LISR AND EXTREME CASES OF THE VARIABLE Z

Zone	Extreme cases	LISR
Z>46.08	Z=64, P1=100%, P2=22.22%	[46.08,64]
Z<46.08	Z=36, P1=56.25%, P2=100%	

In sum, the majority of the TNSSP judge cybercrime, an evolving phenomenon accompanied by a non-scalable legislation.

V NOTICES AND RECOMMENDATIONS

After having chosen the quantitative study axes and criteria to study the human behavior in the face of digital crimes according to the social psychology, we proceeded directly to the realization phase in three steeps (data collection, results presentation, results synthesis). Through this study, we have been able to deduce important remarks concerning the study itself, to discover some bases of the direct and indirect links could relate human behavior to cybercrime and to confirm some impacts of the human factor on the electronic economy:

A. Remarks and Limits of the Adopted Study

- The coherence between some study criteria (for example the study level and age criteria) increases the studied sample quality, which facilitates more the study itself.
- Despite the specific characteristics of the studied geographical area, the fact of meeting within it, during the study, a considerable number of neighboring areas individuals makes it possible to generalize the study results on the immediate geographical neighborhood.
- It is now necessary to perform, in a second phase, a complementary psychological study in the field of cybercrime. This study will allow, on the one hand, discovering the global impact of the human psychological components on the cybercrime study and, on the other hand, discussing the possibility of developing, based on our study, a theoretical and/or practical model that links between social psychology and the cybercrime field.

B. Links between Human Behavior and Cybercrime

- The ignorance is a powerful source of cybercrime: ignorance of the computer security importance, ignorance of the DW risks, ignorance of cybercrime legislation, etc.
- The audacity to perpetrate crimes multiplies from the real world to the DW.
- The victims of the DW are most likely unfamiliar.
- The knowledge of the DW victims increases the level of vigilance when using digital services.
- The increase of the study level leads to the increase of the vigilance degree in the use of the DW services.
- The increase of the study level increases the conviction that the computer security tools, used to counter the DW risks, are necessary but insufficient.
- The increase of the study level means the increase of the individual comprehension level but it does not imply the increase of the degree of the individual consciousness and maturity, especially in the DW.

- The absence of both awareness and responsibility makes the familiarization with the DW, which is strongly linked to the increase in the study level, a real threat to the DW.

C. Impacts of the Human Behavior on the Digital Economy

- The lack of familiarity with the DW has a negative impact on the profitability of digital services such as e-commerce, digital marketing, etc.
- The remarkable increase in the audacity of perpetrating crimes during the transition from the real world to the DW certainly threatens the digital economy.

VI Conclusion

Generally, the relationship human factor-cybercrime is multidimensional and its consideration in the cybercrime study is important to clarify the manner to use effectively the human behavior in the fight against digital crimes. In short, it is extremely important to know for each studied population its dominant characteristics (attitude, intention and behavior) in order to decide on its management and control policies/strategies.

To conclude the present study, on the one hand, we extended the human attitude criteria by adding, to these study basic criteria (age, study level and origin city), two new criteria (knowledge and qualification) and, on the other hand, we limited to three dimensions (Fig. 8).

- Vertical dimension (some attitude components and behavior): The attitude criteria all evolve positively from bottom to top. On the one hand, the age and study level criteria increase, in a consistent way, in this direction and, on the other hand, the knowledge (security, legislation, etc.) and the qualification (computer tools mastery, capacity of e-commerce actions, etc.), which depend on the three basic criteria, also evolve positively upward from ignorance to knowledge and from non-qualification to qualification, respectively. This dimension also illustrates from which study level could start appearing other attitude criteria.
- First horizontal dimension (interactivity Attitude-behavior-cybercrime): This dimension illustrates the links that could relate the human being, based on his attitude and intention, to a specific behavior inside the cybercrime area; namely a digital criminal or a WD victim.
- Second horizontal dimension (fight against cybercrime): The main activities of the fight against cybercrime, that can be undertaken based on the human behavior, begin with the training and sensitization (ethics, deontology, etc.) in academic environments followed by the watch (monitoring, measurement, etc.) to be able to anticipate and develop the adequate action strategies. Finally, we find the action which includes all the possible used tools and/or platforms (technical, legislative, etc.) to, on the one hand, protect the human behaviors victims of the cybercrime and, on the other hand, to fight against the human behaviors constitute digital malefactors (blocking, arrest, etc.).

In the future, we will carry out, in the future second phase of this study, a quantitative psychological study that will enable us to further deepen our knowledge in this psychological aspect of cybercrime and to continue developing this important axis of the cybercrime field.

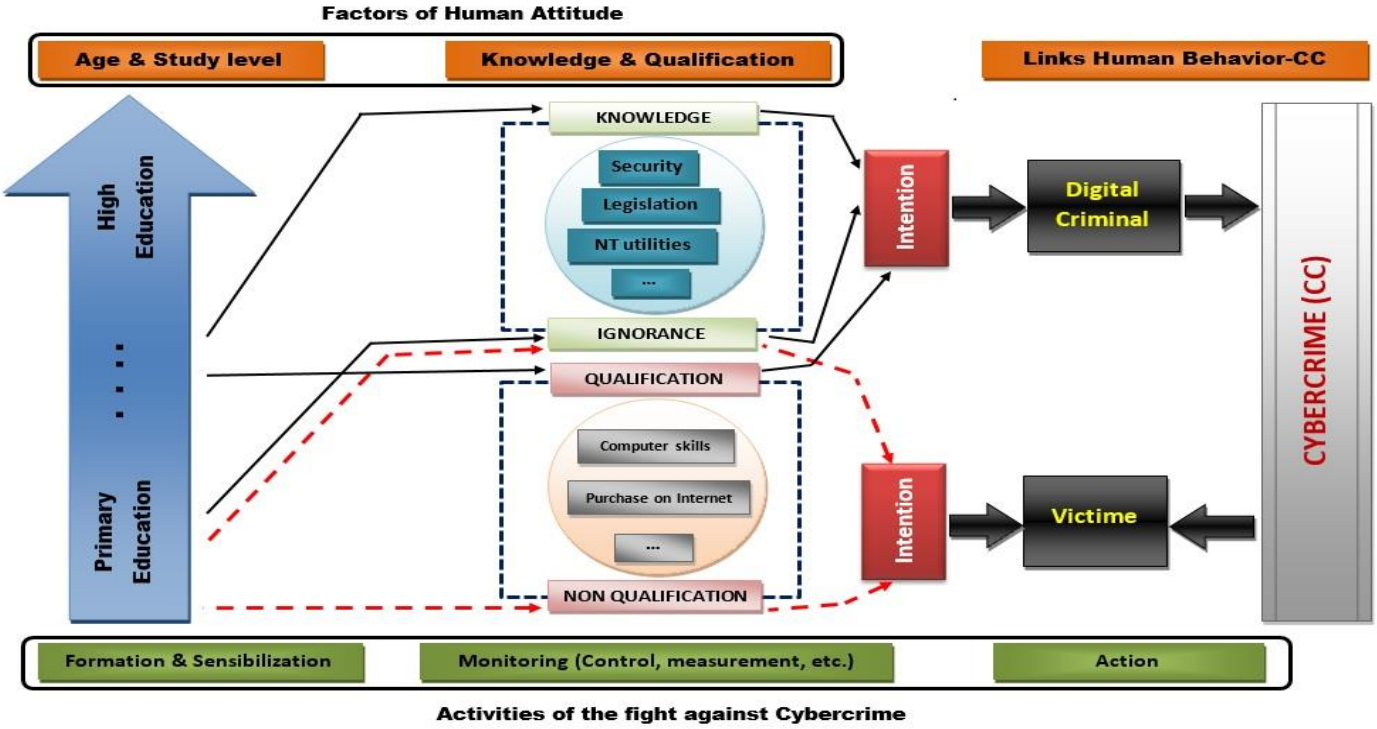


Fig. 8. Schematic Representation of Possible Links between Cybercrime and Human Factor.

ACKNOWLEDGMENT

Our sincere thanks to the ENCG-J students, whose names are listed below in alphabetical order, for their participation in the realization of our field study: ACHIR Chaimaa, BAHRI Hajar, BENIOURI Hamza, BOUZIANE Abdelmounim, MAZOUI Asmae, SABRI Sanaa and RAVELONARIVO Ny Harimirana.

REFERENCES

[1] M. Lagazio, N. Sherif and M. Cushman, "A multi-level approach to understanding the impact of cyber crime on the financial sector," Computers & Security, Elsevier, vol. 45, pp. 58–74, 2014,.

[2] N. Kshetri, ''The simple economics of cybercrimes," IEEE security & privacy, vol. 4, issue 1, pp. 33–39, 2006.

[3] A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," Procedia Economics and Finance, vol. 28, pp. 24-31, 2015.

[4] S. Gordon and R. Ford, "On the definition and classification of cybercrime," Journal in Computer Virology, vol. 2, issue 1, pp. 13–20, 2006.

[5] H. Orman, "The Morris worm: a fifteen-year perspective," IEEE Security & Privacy, vol.1 , issue 5 , Sept-Oct 2003.

[6] R. Solms and J. Niekerk, "From information security to cyber security," Computers & Security, vol. 38, pp. 97–102, October 2013.

[7] L. Tabansky, "Critical Infrastructure Protection against Cyber Threats," Military and Strategic Affaires, Vol. 3, no. 2, Nov 2011.

[8] A. Arabo, "Cyber Security Challenges within the Connected Home Ecosystem Futures," Procedia Computer Science, vol. 61, pp. 227–232,2015.

[9] H. de Bruijn and M. Janssen, "Building Cybersecurity Awareness: The need for evidence-based framing strategies," Government Information Quarterly, vol. 34, issue 1, pp. 1-7, January 2017.

[10] R. Broadhurst, P. Grabosky, M. Alazab and S. Chon, "Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime," International Journal of Cyber Criminology, vol. 8, issue 1, pp.1–20, January - June 2014.

[11] C. Dejours, "Le facteur humain," Collection Que sais-je ?, 6th edition, 2014.

[12] K. Janssens, N. Nijsten and R. Van Goolen, "Spam and Marketing Communications," Procedia Economics and Finance, vol. 12, pp. 265-272, 2014.

[13] C. Williams, "Security in the cyber supply chain: Is it achievable in a complex, interconnected world?," Technovation, vol. 34, issue 7, pp. 382-384, July 2014.

[14] M. Antonescua and R. Birau, "Financial and non-financial implications of cybercrimes in emerging countries," Emerging Markets Queries in Finance and Business, Procedia Economics and Finance, N32, pp. 618 – 621, 2015.

[15] M. Lagazio, N. Sherif and M. Cushman, "A multi-level approach to understanding the impact of cyber crime on the financial sector," Computers & Security, vol. 45, pp. 58-74, September 2014.

[16] Kanich C, Kreibich C, Levchenko K, et al, "Spamalytics: an empirical analysis of spam marketing conversion," Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS), pp.3–14, 2008,

[17] K.T. Smith, L.M. Smith and J.L. Smith, "Case studies of cybercrime and their impact on marketing activity and shareholder value," Academy of Marketing Studies Journal, vol. 15, num. 2,pp. 67-81 ,2011.

[18] C. Nuangjamnong, S.P. Maj and D.R. Veal, "The OSI Network Management Model - Capacity and performance management," Proceedings of 4th IEEE International Conference on Management of Innovation and Technology. ICMIT 2008. Bangkok, Thailand. IEEE, pp. 1266-1270, 2008.

[19] Marc D. Goodman and Susan W. Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace," International Journal of Law and Information Technology, vol. 10, No. 2, 2002,

[20] E.F.G. Ajayi, "Challenges to enforcement of cyber-crimes laws and policy," Journal of Internet and Information, Systems, vol. 6, num 1, pp. 1-12, August 2016.

[21] S.M. Young, "Verdugo in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases," 10 Mich. Telecomm. & Tech. L. Rev. 139 (MTLR), vol. 10, issue 1, 2003.

[22] M. Fishbein and I. Ajzen, "Attitudes towards objects as predictors of single and multiple behavioral criteria," Psychological Review, vol. 81, Num .1,1974, pp. 59-74, 1974.

[23] I. Ajzen, "The theory of Planned Behavior," Organizational behavior and Human Decision Processes, vol. 50, pp. 179-211, 1991.