Using Fuzzy Similarity Measures to Assess the Factors Disposed to Commit Cyber-Crime

Ezer Osei Yeboah-Boateng
Ag. Head (Dean), Faculty of Informatics, Ghana Technology University College (GTUC), Accra, Ghana

eyeboah-boateng@gtuc.edu.gh, ezer@ezitech.net

ABSTRACT

This exploratory study examines the characteristic attributes that predispose patrons to commit cyber-crimes. Cyber-crime is nicknamed as “Sakawa” in Ghana, which involves the use of Internet-enabled PCs, equipped with webcam, and a user with basic computing skills of sending and receiving emails and/or instant messaging. Interestingly, patrons have mastered the “non-monetary currencies” framework to woo their unsuspecting victims. False representations are made to defraud or induce victims to deliver anything valuable or convertible to credit. What motivates patrons to engage in this infamous trade? How could patrons be persuaded to cease operations or disengage from this fraudulent trade? This study relied on expert knowledge elicited through various interviews and followed up with a survey on the mindset of the patrons. Cognizance of the fuzzy nature in profiling perpetrators, fuzzy multi-attribute decision-making (MADM) approach was employed to examine the factors that may influence or predispose a person to commit cyber-crime. Using fuzzy similarity measures analytics, taxonomy of criminal behavioral characteristics were ranked. The study revealed that key attributes of being apt to “cheating”, having an attractive “opportunity” and lack of “friendship” are factors highly possible to predispose a patron to commit cyber-crime. The study also indicates that perpetrators are mostly young males under 29 years, motivated by monetary gains, with the skills to utilize anonymous proxies, taking advantage of difficulties associated with cross-border investigations, apprehension and prosecution. Finally, the results indicate that if some form of stipend or a job were offered the patrons, almost all of them would leave the trade and take up more fulfilling challenges in society.

Keywords: Cyber-crime, Fuzzy Similarity Measures, Multi-Attribute Decision-Making, Perpetrators, Cyber-victim

1. INTRODUCTION

This is an exploratory study on the factors or characteristic attributes of cyber-crime perpetrators, in respect of their predisposition to commit crimes, using Ghana as a case example. In Ghana, the infamous cyber-crime, which has assumed its highest patronage amongst many youth, is nicknamed “Sakawa”.

The Sakawa menace is usually patronized by the youth (over 85% of patrons are under 29 years). It involves the use of Internet enabled PC or laptop, and equipped with a webcam, with little knowledge on using computers. The patron ought to know how to send and receive email messages; and probably to use instant messaging applications, such as what’s app, twitter, Instagram, etc. The modus operandi follow notable knowledge management framework of six (6) non-monetary currencies used in defining and shaping relationships [1, p. 3]. The key constructs are attention, information, association, service, loyalty and advocacy.

First, the perpetrators endeavor to get the attention of the would-be victims (their customers), and then exchange some information with the would-be-victims. Over a period of time, this relationship is developed into an association, where the perpetrator and victim relate in a cordial manner. Now, perpetrator and/or victim begin(s) to offer some form of services, by way of exchanging intangible assets like advice and sharing of concern as perpetrator engages victim emotionally. This relationship develops into offering more tangibles services such as gifts and money as loyalty is developed. It would not be long before the victim becomes an “advocate” of the perpetrator by introducing him or her to other family members or friends. Sometimes with the intent to get married or assisting the perpetrator to visit the victim’s home or domicile country. Interestingly, [1] notes that though the bottom-line – money, is not part the relationship capital, it is a possible outcome of a successful relationship.

The approach notwithstanding, there are variants of this cyber-crime. One form is the popular advance-fee fraud in which the target is persuaded to advance relatively small sums of money in the hope of realizing a much larger gain. Among the variations of this crime is the Nigerian Letter (or 419 frauds), which is derived from the Nigerian criminal code, chapter 38 – “obtaining property by false pretences: cheating”, article 419. This involves the use of any representations made using computing resources, either in words or writing, which are false in fact. This false pretense is applied to defraud or induce victims to deliver to the perpetrator anything valuable or convertible as credit.

It must be noted that almost all patrons in the Sakawa trade are motivated by financial gains. Generally speaking, a small percentage of this cyber-crime is committed locally, that is, with a victim in one’s own country. Majority of cyber-crime crosses jurisdictional boundaries and in view of the anonymity of the Internet, it is very difficult for investigation, apprehension and prosecution. Amazingly these patrons have learnt to use anonymous proxies thus making forensic auditing and tracking (trackback) cumbersome and thereby fueling the patronage, especially when they perceive that identification and apprehension is a herculean task.
Patrons either disregard the governing laws in their countries and/or they rationalize that those laws may not be applicable to them. Though the situation is worrisome, the law enforcement agencies world-wide are collaborating with forensic experts and researchers to fight this cyber-crime. Research works such as this provides invaluable insights into their operations and this project seeks to offer some insights into their mindset and attributes, as well as to assist policy-makers to initiate programs aimed at redirecting the talents and skills of these young people’s into more useful areas in society.

Here we seek to examine some peculiar attributes used in profiling youthful perpetrators, such as cheating, drug abuse, lack of family support, lack of friendship, insecurity, and other key motivational factors in luring someone to commit cyber-fraud. Typically, the attributes are multivariate and fraught with a lot of uncertainties. Thus, conventional descriptive statistics may not be enough to model the uncertainties involving cyber-crime as we attempt to sample views, opinions or collect data from the people breaching the laws of a country and the international community. Principal component analysis (PCA) as a tool was used to deal with the multivariate aspects and to bring out the structure and similarity of latent variables or characteristics.

It must be noted that the concepts or attributes being examined here in respect of profiling the perpetrators are all fuzzy concepts by nature. For example, that someone is apt to “cheat” is subjective. To what extent does he cheats. Similarly, a drug abuser might be using the drugs daily, or once a week or once in a while.

Using fuzzy linguistic variables, derived from expert knowledge, greatly enhances the analysis of this cyber-crime profiling by employing both intuition and human reasoning. The concept of cyber-crime profiling is too complex to use a traditional approach. Fuzzy logic is highly useful for problems of this nature where mathematical modeling may not be feasible due to data unavailability or incomplete datasets.

Due to the delicate nature of collecting data from crime perpetrators, the dataset is small and may not be feasible to draw general conclusions. They, however, provide insights into their mindset and characteristic attributes and to present policy-makers with an opportunity to explore further measures in fighting this menace.

In dealing with the uncertainties and fuzzy aspects, we adopted the fuzzy similarity measures analytics as a means to characterize the attributes that may influence or predispose a person to commit cyber-crime.

This paper is organized as follows: In the following section we highlight on the key motivations for this research and the research questions. We then review related works in the areas of cyber-crime profiling and social theories alluding to perpetrator characteristics, and multi-attribute decision making (MADM), using fuzzy similarity measures analytics. It is followed with the methodology applied in collecting and analyzing our data sets. We also gave some insights into the operations of Sakawa as it pertains in Ghana. We discussed the empirical results and analysis, and based on some inferences we drew conclusions.

1.1 Key Issues – Motivation & Problem Formulation

Lots of young Ghanaians patronize in Sakawa. They are enticed by the monetary gains and the anonymity of the Internet. Apart from tainting the hard won image of Ghana as a destination for the golden age of business in sub-Saharan Africa, it can also inhibit the efforts to promote e-commerce, to attract tourism and stifle economic growth.

By investigating and getting to some basic attributes which are likely to dispose a patron to commit cyber-crime, policy makers can effectively mitigate the menace and most importantly, to re-channel and harness the youthful human capital into more productive social contributors. This study can also assist and inform law enforcement agencies about the profiles of cyber-crime perpetrators.

The key motivating factors for this research are:

- What are the main attributes of cyber-crime perpetrators?
- What are the key motivations of engaging in cyber-crime?
- What can motivate a successful cyber-crime patron to cease operations or disengage the fraud?

In order to appreciate the key motivations of cyber-crime perpetrators, we needed to examine their mindset and understand their profiles, as well as ascertaining whether they have reusable skills or not. We also needed to understand the perpetrators ever-evolving methods of operation, including an attempt to identify some exploitable technologies.

2. RELATED WORK

Cyber-crime in criminology is not entirely a new phenomenon. Rather, the definitions and ever-evolving methods employed have introduced lots of uncertainties in cyber-crime investigations. Cyber-crime is typically trans-national and borderless, which makes detection and apprehension a daunting task.

Some definitions and authorities perceive cyber-crime as crimes or activities or violations committed by the use of computers, either as tools, targets, or with networks [2] or crimes against data or content [3], or fraudulent acts, including unauthorized access to computer systems [4].

For this study, we define cyber-crime as any act of violations or commissions that use or require the use of
computers and its associated systems to either carry out the act or as a tool in aiding the said violations, or targeting the computers systems as well as requiring computers in the investigations.

2.1 Profiling the Cyber-criminal

Generally, a crime can only be committed if certain actors are in operations. That is, it requires a perpetrator with adequate motive to commit crime, and that there is a victim or target, as well as the absence of any deterrent (e.g. a police or a punitive reward) [5][6].

The key motivation of committing cyber-crime is monetary, though there are some who may have ulterior motives. It’s now common place to find and buy destructive tools online to ply their cyber-crime trade [7].

Messrs. Akamai Technologies [7] posit that the rewarding prospects coupled with low entry barriers and low risk involved with the trade, has increased the patronage in cyber-crime in recent years. In some instances, the patrons have developed high tolerance for risk and often rationalize their actions.

There are scanty research works on cyber-criminal profiling and discovery of the different methods that perpetrators employ in their modus operandi [8].

According to a renowned certified forensic expert, Nick Brignola, three (3) traits are present within the mindset of every fraudster. These are perceived need, perceived opportunity and rationalization of behavior [9].

Another expert, Lisa Eversole identified the following characteristics with fraudsters – usually male; intelligent; risk taker; rule breaker; greedy; financial need; overwhelming desire for personal gain; and pressure to perform, among others [10].

Social Positivism postulates that “societal factors such as poverty, membership of subcultures, or low level of education can predispose people to crime” [11]. Social Positivism (originally postulated by Emile Durkheim, 1895) seeks to deepen the understanding of criminal origins and to provide legitimacy for external factors influencing individuals to commit crime. It argues that society is dynamic and respond to social inequality and social conflict. Adolphe Quetelet made use of empirical data and analysis to explain the correlation between crime and sociological factors. He discovered that “age, gender, poverty, education and drug abuse (alcohol) were important factors related to crime” [12].

Space Transition Theory (STT) postulates that persons in good societal standing or position, are likely to repress their criminal behavior in physical space, but are highly disposed to commit crime in cyber-space [13]. In essence, a person’s concern for one’s status on physical space is not transition to cyber-space. Jaishankar posits that the dissociative anonymity in cyber-space gives people (especially victims) the platform to open up to strangers about their personal issues. He continues that perpetrators rather become less altruistic; more selfish and more aggressive in cyber-space. STT argues that persons from closed society are more likely to commit cyber-crime than persons from open society. Norms and values in the physical space are not transition into the cyber-space, which is perceived as international. For example, victims are described as “mugu” – to wit “ a fool” in Huasa language, whereas in physical space even strangers are respected, especially in African cultures.

Routine Activity Theory (RAT) developed by Marcus Felson and Lawrence Cohen [5][6], postulates that routine activities may predispose a person to commit crime, when crime opportunity factors converge in time and space. It argues that in the absence of a significant deterrent such as a guardian, a person would utilize any criminal opportunity, as long as the victim routinely comes to the place of convergence; i.e. visit to the Internet. However, in terms of cyber-crime (especially in Ghana), most of the acts are committed from a public access venues (PAVs) or public Internet cafés, some of which are equipped with CCTV cameras.

Whereas opportunity theory argues that an opportunity to commit crime is paramount, the displacement theory seeks to reduce opportunities as a means to control crime. However, research on displacement theory indicates that crime is not always displaced especially in physical space.

Strain Theory (a.k.a. Mertonian Anomie) developed by Robert Merton, postulates that social inequality coupled with societal expectations of prosperity, propels others to turn to illegitimate means (crime) in order to subsist [14]. Yet, others turn to retreat or drop out into deviant subcultures such as drug abuse.

Social Control Theory, developed by Travis Hirschi, proposed four (4) main characteristics that explained why a person may NOT be disposed to commit crime. They are (i) attachment to others; (ii) belief in moral validity of rules; (iii) commitment of achievement; and (iv) involvement in conventional activities [15]. The more a person exhibits these qualities, the less are the propensity for he/she to commit crime [16].

2.2 Fuzzy Multi-Attribute Decision-Making (MADM)

This research deals with non-numerical quantities, for instance “predisposition”, which cannot be measured against a numerical scale. An example of such a universe could be the tuples [not-at-all disposed, slightly disposed, somewhat disposed, very disposed, extremely disposed]. The notion of fuzzy sets is highly intuitive and transparent as it captures the essence in which a real world is perceived and described [17]. The fuzzy logic theory is just a prolongation of traditional logic where partial set membership could exist, rule conditions could be satisfied partially, and system outputs are calculated by interpolation.
We reckon that any viable or effective approach used in analyzing the multi-faceted cognitive characteristic factors that pre-dispose patrons to commit cyber-crimes, is one of fuzzy multi-attribute decision-making (MADM).

This approach is employed to analyze and rank cyber-crime characteristic attributes as perceived by the sample experts as influential factors likely to predispose patrons to commit crime. The objective is that given a set of attributes deduced from the study of behavioral alternatives, then fuzzy MADM techniques are used to analyze and rank them in the order of most-to-least influential factors.

It is noted herewith that this study chose to use fuzzy triangular numbers, for simplicity and ease of computation. For instance, it can be showed that similar treatment with fuzzy trapezoidal numbers would yield similar results.

Fuzzy Similarity Measures is a basic concept in human cognitive assessment. In literature, it is also referred to as degrees or measures of similarity. It finds various applications in multi-attribute decision-making (MADM), fuzzy ordering or ranking, such as taxonomy, recognition, case-based reasoning, etc. [18]. In this study, fuzzy similarity measures is utilized in the analysis and ranking of the influential factors likely to predispose patrons to commit cyber-crime.

Generally, similarity measures are categorized into three (3) types, which are metric-based measures, set-theoretic based measures, and implicators based measures [18]. This study utilizes an aspect of the set-theoretic based similarity measures and focuses on fuzzy similarity measures.

2.3 Internet Proxies & Anonymity

A proxy server is a network device that serves as an intermediary or a conduit between an end-user and various Internet resources, such as websites, cloud based applications, Instant Messaging (IM), electronic transactions, etc. Requests made by the end-users on the Internet are passed onto the proxy server, which in turn relays the requests and exchanges the received responses. In essence, the end-user connects to the Internet indirectly through the proxy serve. Proxies enable end-users to mask their original public IP addresses in order to ensure that their online identities are undetected.

An anonymous proxy server, also known as “anonymizer”, therefore, is a special purpose proxy that is utilized to mask the end-user’s IP address during transactions and substitutes with that of the server. Typically, most proxy servers are identifiable on the Internet, but they may mask or submit incorrect end-user IP address. A high anonymous proxy server, also known as elite proxy server, is the type which masks both the server IP and that of the original end-user.

In practice, there are lots of high anonymous proxies which are web-based, and ranging from being free to a few dollars. A disadvantage in using proxies could be transactional delays or high latency. Incidentally, most cyber-criminals understand the workings and benefits of anonymous proxies, and prefer to hide their original IP addresses, in order to carry out their nefarious activities. Using a proxy server has become so easy, as no third-party software may be required; just a web browser and Internet connectivity.

It must be noted that the use of anonymous proxy servers could be for legitimate purposes. For instance, end-users would connect via anonymizer to conceal their identities (for privacy concerns), such as pop-ups, cookies, and to by-pass Internet censorship or regime repression. Here, the anonymizer is used for solely to circumvent Internet restrictions and to protect the end-user’s privacy.

3. METHODOLOGY

In designing the empirical study, we reviewed relevant literature and theories on cyber-crime and profiling of youthful criminals. We also conducted expert interviews with cyber-café owners and some patrons.

The expert knowledge acquired through observations and interviews were used to inform the nature of survey questionnaire administered. We then subjected the dataset into various analyses such as basic descriptive statistics to find out demographics of patrons, and we used the UNSCRAMBLER X.10.1 principal component analysis (PCA) to confirm the expert knowledge from interviews in respect of the key attributes.

Our output question in the survey was: “if you were offered a stipend or a job or some subsidy, would you still engage in Sakawa?” Five (5) linguistic terms were offered as possible answers, of which respondents chose one (1) suitable answer. In view of the fuzzy nature, and for simplicity, we used fuzzy triangular numbers (FTN) for the linguistic terms. The fuzzy approach deals with the uncertainties and vagueness in human reasoning, as well as resolving the subjectivity in this complex real-world problems of cyber-crim. The factors or attributes were then evaluated using fuzzy similarity measures to assess the extent of influence that a particular attribute may have on predisposition of perpetrators to commit cyber-crim.

3.1 Data Collection Procedure

Five (5) cafés were approached randomly, but only three (3) cafés agreed to patronize in the survey. The study administered an objective-based structured questionnaire to 150 cyber-crime and cyber-café patrons in Accra, Ghana. During pre-survey interactions café owners were debriefed on the purpose of the study and so identified patrons were actually surveyed. Out of that, 67 respondents were received and analyzed, and those constitute the findings in this paper.
3.2 Principal Component Analysis (PCA)

Principal Component Analysis (PCA) is a way of identifying patterns in data, and expressing the data in such a way as to highlight their similarities and differences. Since patterns in data can be hard to find in data of high dimension, PCA becomes a powerful tool for analyzing data [19].

We administered a questionnaire of fifteen (15) items which represents 15 variables of interest. Since some of the variables may be measuring the same construct and so correlate with each other, by using PCA, we reduced the number of variables to five (5) key variables without much loss of generality or information.

The PCA identified the various correlated patterns amongst the variables. We observed that five key variables had more loadings or influence than the others and also conformed to the expert knowledge and literature. We then used these 5 variables as predictor or criterion variables or attributes in fuzzy similarity measures analytics.

3.3 Data Limitations & Challenges

As expected it was not an easy task getting crime perpetrators to agree to speak with the researcher and associates, especially when the interview ought to be recorded and notes taking. Collecting the data took longer than usual because the café owners had been assured that this was an academic exercise and NOT a police undercover investigations. Once the trust of the café owner was earned, it facilitated the introduction of some patrons and also permitted the use of the café facility for research purposes.

3.4 Cyber-crime in Ghana (Sakawa)

Sakawa is a form of cyber-crime which involves mainly identity deception and other aspects of social engineering. In some cases they employ identity theft when they procure stolen personal information or credit cards [20][21].

Sakawa is alleged to be practiced with some occultic aspects, which is purported to aid in manipulation of the unsuspecting victims into acceding to the perpetrator’s demands under coercion [22]. The caveat here is that, this paper merely treats Sakawa in the context of physical and tangible computer systems and their operations. Anything outside of that is beyond the scope of this study.

According to [23], “the perpetrators’ intent and purpose is to get to the targets’ money, goods and services (assets), or avoid costs and expenses (liabilities), and evade detection or blame through the use of another’s legitimate identification account channel with the target”. The patrons are perceived as cyber-punks and socially inept [24], but they are smart and apt for multi-tasking. They usually engage a number of victims simultaneously and flatter their victims to gain their trust. They talk a lot but offer vague answers and sometimes interjects with useless jargons.

4. EMPIRICAL ANALYSIS & RESULTS

4.1 The Data

The datasets were pre-processed using the UNSCRAMBLER 10.X, which also aided in uncovering the latent principal components and their correlations. The datasets for this study are organized as matrices or arrays of numbers representing the fuzzy linguistic terms or tuples.

The key parameters in the study were as follows:

- a. Age – as part of demographics to ascertain whether indeed the patrons are youth or not;
- b. Usage – as part of demographics to ascertain the extent of patronage;
- c. Motivation – as part of demographics to ascertain what are the drivers that led patrons to computers and Internet;
- d. Opportunity – as the extent of attractiveness of the target and thrill of not being caught; it also include necessary tools and/or facilities needed to engage in the trade and its availability;
- e. Skill set – as the necessary level of technical expertise or education required to engage in the trade;
- f. Key Motive – as the primary goal for patronage;
- g. Success rate – as an indication of the level of achievement in the trade;
- h. Insecurity – as a key variable indicating the extent of insecurity entertained by patrons;
- i. Friendship – as a key variable indicating whether patrons are loners or enjoy any friendship;
- j. Family Support – as a key variable indicating the extent of family influence or the lack of it on patrons;
- k. Cheating – as a key variable indicating the extent to which patrons are able to cheat or as an indicator of the ease with which patrons can cheat and its correlation to involvement in identity deception;
- l. Drug Abuse – as a key variable indicator ascertaining the influence or otherwise of drug use on cyber-crime;
- m. Stipend – as a key variable indicator and an output variable, used to ascertain whether or not patrons are likely to leave the trade in lieu of a subsidy or a stipend or when offered a socially acceptable income generating activity.

4.2 Key Indices

This section outlines the key indices of investigating the mindset and characteristic attributes of Sakawa patrons. It has been structured as three (3) objectives aimed at understanding the underlying factors that drive energetic youth into cyber-crime, as well as to ascertain if these factors or attributes predispose patrons to commit cyber-crime. We don’t presume that our findings are a panacea to solving cyber-crime in any
developing economy, but as an attempt at suggesting some ways in which policy makers may create opportunities for these disadvantaged youth. It is also aimed at assisting law enforcement agencies in profiling the cybercrime perpetrators.

The 3 areas leading the discussions are:

a. To appreciate the main attributes of cyber-crime perpetrators;
b. To understand the key motivations of engaging in cyber-crime;

c. To appreciate the extent of the cyber-crime menace and to propose mitigating measures to solve the problem.

### 4.3 Fuzzy Similarity Measures Analytics

Now, let the fuzzy linguistic variables be defined by the tuples $S = \{s_j : i = 1, 2, \ldots, n\}$ such that $s_i < s_j$ iff $i < j$.

In this study,

$$S_{(R_i, R_j)} = S_{A, B} \leq \varepsilon.$$

Another useful method is that of Xu [27] for similarity measure given by

$$S_{(R_i, R_j)} = 1 - \frac{|a_2 - a_1| + |b_2 - b_1| + |c_2 - c_1|}{8q} \quad (3)$$

Where $q = 3$ for fuzzy trapezoidal numbers and $q = 4$ for fuzzy trapezoidal numbers.

It is noted that

$$S_{(R_i, R_j)} \in [0, 1]$$

and $S_{(R_i, R_j)} \rightarrow 1$ implies that $R_i$ and $R_j$ are closer to each other. So

$$S_{(R_i, R_j)} = 1 \text{ iff } R_i = R_j \text{ and that also } S_{(R_i, R_j)} = S_{(R_i, R_j)}$$

Assume that the fuzzy set $X = \{x_1, x_2, \ldots, x_n\}$ is the set of alternatives and $U = \{u_1, u_2, \ldots, u_m\}$ be the set of influential characteristic attributes. Then for a given degree of importance or weights vector $W = \{w_1, w_2, \ldots, w_m\}; \forall w_i \geq 0; i = 1, 2, \ldots, m.$

the linguistic decision matrix or agreement fuzzy matrix (AM) is computed as

$$AM_{mn} = \begin{bmatrix}
S_{11} & S_{12} & \ldots & S_{1n} \\
S_{m1} & S_{m2} & \ldots & S_{mn}
\end{bmatrix} \quad (4)$$

### Degrees of importance can be computed from the equation

$$W_i = \frac{r_i - \mu_i}{\sum r_i} \quad (1)$$

For any given fuzzy sets $A = \{a_i\}$ and $B = \{b_j\}, \forall i = 1, 2, \ldots, n$, the grade of similarity (or agreement degree) of the fuzzy relations is given by

$$S_{(R_i, R_j)} = \frac{\sum (a_i \land b_j)}{\sum (a_i \lor b_j)} \quad (2)$$

Equation $[eqn-2]$ is known as the min-max similarity method [25], and the fuzzy sets A and B are said to be approximately equal if and only if (iff), there exists a proximity measure, $\varepsilon$, [26] such that
In most techno-economic researches, the significance level is set at $\leq 0.05$, and we have chosen 0.05. In statistical terms, we say that the observed outcome is statistically significant if the probability of the difference occurring by chance is less than five times out of a hundred (i.e., we conclude that something else other than chance has affected the outcome). [28]. The results are used in examining, explaining, confirming, refuting, and/or enriching information from the literature and expert knowledge.

Using the 3-point criteria, we deduce as follows:

a. What are the main attributes of cyber-crime perpetrators? The Fuzzy Similarity Measures generated taxonomy of attributes that are most influential factors predisposing cybercrime perpetrators to commit the crime. Key amongst the attributes is cheating, opportunity and friendship.

b. Statistically, 90% off the samples had little or no difficulty at all cheating, with only 5% that found it very difficult to cheat. Literature supports this attribute as being an influential factor in predisposing a person to commit crime [29].

The opportunity attribute presents the extent to which resources are available to carry out the trade, as well the attractiveness of the target. Included in this attribute is the thrill and/or belief they would never be caught or the laws do not apply to them.

The friendship attribute connotes lack of friendship and/or the presence of delinquent friends, instead. Statistically, 34% had no friends at all, 46% just a few friends, and only 5% had many friends. These include marital discord, family discord, low parental care, low family ties, etc. Criminological literature is consistent and strong on the correlation between influences from delinquent friends and criminality [30]. It must be noted that, these influential factors are not necessarily causative factors, they however, correlate with the frequency of crime behavior and merely suggest the possibilities of crime perpetration.

We hereunder present an overview of some descriptive statistics from the study:

- 86% of respondents are under 29 years and 21% are teenagers, with just 1% over 40 years;
- 79% use the Internet very often or often, whilst 19% use it once awhile;
- 55% had used drug at least once, 31% use drug often or very often, with only 4% never tried drugs;
- 46% had no family support at all, 49% had inadequate or very small family support, only 5% had sufficient family support;
- 75% are either insecure or very insecure; whilst only 10% really feel secured;

We infer that most of the attributes of cyber-crime perpetrators are in support of the various theories...
and expert knowledge, especially those regarding cheating, drug abuse, lack of friendship, insecurity and lack of family support.

c. What are the key motivations of engaging in cyber-crime? Overview of descriptive statistics indicate that:
   - Key Motive – as expected 75% admitted that the key motive was money, whilst 10% said curiosity or power, and only 5% for revenge. Interestingly no one opted for intellectual prowess as their primary motive;
   - Success Rate – 95% had succeeded in the trade at least once of very often; whilst only 2% had never been successful.

d. What can motivate a successful cyber-crime patron to cease operations or disengage the fraud? Asked whether patrons would continue or cease operations should they be offered a stipend, a subsidy or a job, here were their responses:
   - Stipend – 79% indicated that they would never continue with the trade, whilst 6% indicated they may continue, and only 3% were definite to continue in spite of a stipend.

5. DISCUSSIONS & CONCLUSION

Frederic [31, p. 7] defines a professional fraudster as that individual who is “so smart that had his talents been applied honestly he could probably have been a successful Fortune 500 CEO”. For as long as there is money to be made, some will turn to crime online: when it comes to people, there really is nothing new under the sun.

The key constructs for this study had been fuzzy psychological continuum which sought to prefer some characteristics to persons who may be predisposed to commit or engage in cyber-crime. These “qualities” were subjective human thinking and fuzzy in nature. Thus we used fuzzy logic and linguistic human reasoning to analyze the empirical datasets.

The use of PCA highlighted and gave credence to the research notions and then collaborated related works and theories on profiling cyber-criminals. Using fuzzy multi-attribute decision-making (MADM) and fuzzy similarity measures analytics, the problem of profiling cyber-crime perpetrators and factors predisposing them to commit the crime were appropriately assessed. A taxonomy of key influential attributes of patrons have been preferred which can assist law enforcement agencies in profiling and combating cyber-crime. Also, the key output fuzzy variable “stipend” seems to suggest that probably the 79% indication that patrons will not go back to the Sakawa trade, may be “fuzzy”.

The above notwithstanding, it is a clear indication that some form of social interventions may be needed to curtail this menace. It is incumbent upon policy makers to continue this exploration and to design a program that will re-channel and harness the youthful human capital into more productive social contributors.

Obviously, the data sets were inadequate to draw firm causative conclusions. More research works ought to be carried out to ascertain that these patrons have some employable skills or find out what could be done to make them productive. Finally, the need for more awareness creation on protecting one’s online identity cannot be over emphasized. “Trust but Verify”.

REFERENCES


Australian Police, Australasian Center for Policing Research, 2005.


