Psychol Stud (October–December 2017) 62(4):386–394
DOI 10.1007/s12646-017-0423-9

RESEARCH IN PROGRESS

A Cyber Phenomenon: A Q-Analysis on the Motivation of Computer Hackers

Ryan Francis O. Cayubit[1] · Kevin M. Rebolledo[1] · Romulo Gabriel A. Kintanar[1] · Angelissa G. Pastores[1] · Alen Josef A. Santiago[1] · Paula Bianca V. Valles[1]

Received: 21 February 2016 / Accepted: 15 September 2017 / Published online: 13 October 2017
© National Academy of Psychology (NAOP) India 2017

Abstract In computer security parlance, a hacker is an individual who actively seeks and takes advantage of flaws and weaknesses of a computer network or system. In recent years, one has seen the rise of hacking, often as a form of protest and retaliation for reasons ranging from political to social, but the question remains as to what really motivates an individual to hack a computer network? Using the Q-method, the study aimed to develop a classification of the motivation of computer hackers. This was done with the use of 43 participants who were subjected to preliminary interviews and the sorting method. The statements from the interviews were categorized that resulted in seven conceptual themes, namely social-positive, social-negative, intellectual gain, self-satisfaction, economic rewards, technological-positive and technological-negative. From these themes, three distinct profiles emerged and were used to describe the motivation of hackers.

Keywords Motivation · Computer hacking · Q-analysis

Introduction

Two important questions linger in the minds of the researchers; we are interested to find out what goes on in the mind of a computer hacker and what are the different motivating factors that push them to do what they do. In answering this question, we recognize that we live in a technologically advanced age, where almost everything can be found in the Internet and where most if not all individuals or corporations have relied on computer systems or networks for information storage. Unfortunately, the advent of this technology also gave birth to computer hackers. They are individuals engaged in a successful or unsuccessful attempt to gain authorized or unauthorized access into a computer network or system for various reasons (Dalal & Sharma, 2007; Hoath & Mulhall, 1998). These highly talented individuals commonly fall into three behavioral categories, namely white hats, black hats and gray hats. According to Gold (2014), white hats are hackers whose main objective is to promote justice and the common good, black hats are those who perform hacking for the thrill of it and operate based on their own rules and may at times be described as dangerous, while gray hackers, also known as ethical hackers, are hackers whose standards fall in between that of the white hat and the black hat. Despite the existence of such a category, Rogers (2002) believe that hackers are not a homogeneous group and establishing a classification about them is essential to understanding their behavior.

According to Hoath and Mulhall (1998), the intention to do something illegal was far from the reasons of some computer hackers when they first started engaging in such an activity. For these people, the reason behind it was more of the need to satisfy one's curiosity about data systems and the obsession to learn much about such systems (Menkus, 1991). However, this seems to have evolved as the said curiosity may have propelled computer hackers to engage in criminal behavior. Over time, many negative adjectives have been used in the attempt to understand computer hackers and the logic behind the things they do. They are viewed as determined individuals with obsessive behavior, excellent memory and social engineering skills

✉ Ryan Francis O. Cayubit
ryanfranciscayubit@yahoo.com

[1] Department of Psychology, College of Science, 3rd Floor Main Building, University of Santo Tomas, Manila, Philippines

who operate in small but loose groups and communicate via bulletin boards (Hoath & Mulhall, 1998). In addition, they seem to have no recognition of any wrongdoing and have expressed little to no concern for the plight of others particularly those affected by hacking (Hoath & Mulhall, 1998). Nonetheless, as previously discussed, not all computer hackers are bad as within their ranks, white-hat hackers exist.

Through the years, researches about hackers have taken two courses. Published materials about hackers and hacking have delved on the technological aspect of the process particularly the hacking techniques. The other area of research is the socio-psychological aspect of hacking; an area that is largely considered in its infancy because the motives behind the acts of hacking are often obscure and need various interpretations (Adam & Ofori-Amanfo, 2000). This is the area where we intend to focus on; we recognize this as a gap in the literature and intend to answer it by conducting an exploratory study that will dwell on examining the motivation of computer hackers.

Contemporary psychology dictates that man's behavior is brought about by one's motivation as it is largely considered as the driving force that compels an individual to do certain things (Fersizidis et al., 2010). These are psychological forces that originate from within an individual's being or beyond and often occur in different forms and in diverse contexts as a result of the interaction between the environment and an individual (Latham & Pinder, 2005). Man's motivation is often described as either intrinsic or extrinsic. According to Deci, Vallerand, Pelletier, and Ryan (1991), intrinsic motivation refers to behaviors that have been engaged or initiated by an individual for their own sake because of the pleasure and satisfaction that will be derived because of their performance, while extrinsic motivation is behavior that has been performed not out of interest but because of the external rewards, outcomes or consequences associated with the said behavior. Aside from this, man's behavior has also been attributed to expectancies and subjective task values. According to Eccles (1983), expectancies pertain to the belief of an individual about his abilities and the use of those abilities that would lead to a task being performed successfully, while task values deal with how important, useful or enjoyable a task is. Despite the existence of this common and general classification of motivation, little is known as to what propels an individual to hack into a computer or computer system with little or no regard for ethics, privacy and laws of a country. This lack of information about their motivation from a psychological perspective stems from the difficulty in obtaining data about hacking and hackers (Adam & Ofori-Amanfo, 2000). Of the little information about their motivation, Möjhrenschlager (1995) and Blatchford (1998) identified curiosity as a common factor in many hackers; what is missing, however, is a more theoretical explanation of their motivation, a gap in the literature that this research will attempt to address. Since motivation is largely subjective and varies from one computer hacker to the next, the researchers intend to use the Q-method in analyzing these subjective views by looking at patterns of commonality in the responses; the end result is an initial classification of motivation unique to computer hackers. The researchers would then use the expectancy-value theory to provide theoretical support to the proposed classification by giving an explanation of the nature of the motivation reported by computer hackers.

Psychological Aspect of Hacking

According to Hoath and Mulhall (1998), hacking is as an act of accessing computer systems without legitimate access, though it did not start out this way, but over time the meaning of the word hacker has changed and has become synonymous with criminal activities. Though not entirely correct, this misinformation has resulted to stereotypes that hinder efforts that could help understand their characteristics and motivations (Rogers & Ogloff, 2003; Rogers, 2006).

The little literature on the psychological aspect of hacking relates to determining and understanding why hackers do what they do. The most common motivation appears to be greed; these are hackers whose activities may be considered criminal, and they often develop programs and methodologies of social engineering to assist cyber criminals (Gold, 2011). In addition, in a study that examined why employees result in hacking the company website of their employers, Bainbridge (1997) found out that the main cause is employee dissatisfaction. Hacking has also been associated with age; according to Yar (2005), a trend seems to be appearing where most computer hackers appear to be youngsters who see hacking as a mode of escape from family or school-related suppressions or problems. Despite the differences in motivation, what is common among computer hackers is anonymity.

Expectancy-Value Theory

In general, the expectancy-value theory explains that man's motivation in performing a certain task is grounded in his expectancies for success and the value that he places on the said task (Wigfield, 1994). Originally developed by Atkinson (1957), the theory has been applied in different settings. Expectancies were originally defined as anticipation that a performance of a task will either be a success or a failure and value as the attractiveness of succeeding or failing in the task (Atkinson, 1957). According to the theory, expectancies drive man's behavior and shape the decisions he makes based on the belief that he would be successful in a particular task. The belief is tied to the concepts of self-concept and efficacy beliefs (Bong & Skaalvik, 2003; Eccles & Wigfield, 2002). Subjective values also fuel man's behavior as it answers the question of whether a man would like to do a certain task or not and the reason why (Wigfield & Cambria, 2010). According to Eccles (1983), there are four categories of subjective values, namely attainment value, intrinsic value, utility value and cost. Attainment value impacts man's identity or the self, while intrinsic value deals with enjoyment or interest in the task (Eccles, 1983). Utility value deals with the usefulness or relevance of the task, and cost takes into consideration the amount of time needed to complete a task and other negative psychological experiences (Eccles, 1983).

Conceptual Framework

Considering the nature of the expectancy-value theory and hacking, the researchers believe that it is a viable framework to explain their motivation. It has been established that computer hackers vary in their motivation and the concept of expectancies and subjective task value can be used to explain its nature and why computer hackers continuously engage in such activities despite the known negative consequences. In applying the theory to the present study, expectancies refer to the belief hackers' hold that they can continuously and successfully hack into computer systems every time they want to. This belief is fueled by their past experiences of successful hacking activities, and when combined with their technical expertise, it can give an impression that they are the only ones who can do it, the result of which is an enhanced self-concept and an increase in efficacy beliefs. Task values are subjective judgments of computer hackers regarding their activities; these are practical in nature and serve as the general motivating factor for them to continuously hack computer systems provided the process and the end result will be of value to them. For example, a gray hacker who hacked a government website in order to air his grievances and support a cause has exercised his subjective judgment by highlighting the utility value of the task. In summary, the researchers believe that the concepts of expectancies and task value can shed light on the motivation of computer hackers from a psychological perspective and use these concepts to develop a new classification of their motivation (Fig. 1).

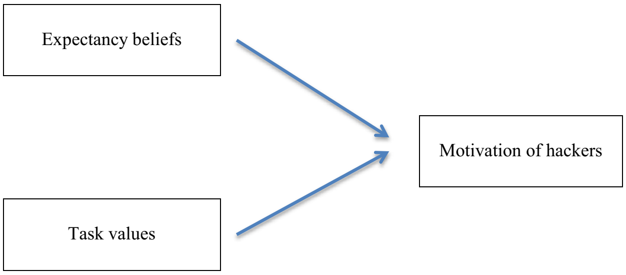

Fig. 1 How expectancy beliefs and task values affect motivation of hackers

Research Objective

This exploratory study intends to show the unique experience of computer hackers. It will look into the specific reasons as to why hackers continue to do what they are doing despite the knowledge of the consequences of their actions. Specifically, it will analyze the motivation of hackers from a psychological perspective using the expectancy-value theory; the result will be a proposed classification that can be used to organize and further understand computer hackers.

Method

Research Design

The Q-methodology was used in order to come up with a new classification for the motivation of computer hackers. It is a systematic approach to research whose main objective is to identify clusters of people based on common viewpoints (Pruslow & Owl, 2012). The design proceeds with the analysis of the different viewpoints of the participants about a certain topic or construct, and clustering is done via the examination of the correlation of the different viewpoints (Dziopa & Ahern, 2011).

Selection of Participants

A Q-study makes use of two sets of participants known as P sets. The first P set is subjected to the initial interview, while the second P set is the group that performs the actual sorting. The number of participants for this type of study is typically low compared to other methodologies as the focus of the study is more on the quality of experiences or key opinions of the participants rather than the generalizability of the results (Cross, 2005; Dziopa & Ahern, 2011).

For the current research, a total of 43 male computer hackers with a mean age of 27.50 y participated, 20 for the first P set and 23 for the second P set. They were all selected via expert sampling since the researchers were after individuals with specific skills or expertise related to computer hacking (Lavrakas, 2008). The participants were self-confessed hackers belonging to an organization. The researchers exerted effort to secure more demographic information about the respondents in order to present a clearer picture of their profile; unfortunately not much information is available about the participants due to the confidentiality agreement entered into by both parties before the start of the research.

Instrumentation and Data Collection Procedure

Phase 1: Interview Stage

The first P set ($n = 20$) was subjected to the initial interview. The interview was done individually and lasted between 20 and 30 min per participant. The goal of this stage was to elicit their views, opinions and answer the central question of what motivates hackers. Their responses were analyzed, interpreted and categorized to clearly define the Q-concourse, a technical concept in any Q-study that pertains to the general theme and concept of the responses in the initial interview (Raje, 2007; van Exel & de Graaf, 2005). The Q-concourse serves as the basis of the 60 statements, known as the Q-sample, which was used in phase 2 of this research. Table 1 presents the major conceptual themes, their descriptions and corresponding statements.

Phase 2: Sorting Stage

All 60 statements or Q-sample were printed on small cards, and the Q-sort table (see Fig. 2) was readied for sorting. The second P set ($n = 23$) individually sorted the Q-sample based on the instruction to arrange the statements using a scale of 1–11 as a guide, where 11 indicates the strongest agreement that that particular statement accurately reflects the motivation for hacking, while 1 indicates the least agreement. The average time for sorting is 25 min.

Ethical Considerations

Considering the nature of computer hacking and possible consequences, should the identity of the participants be revealed, careful planning was undertaken before the start of the research. For both phases, an informed consent was readied and secured from every single participant. The document contains the main purpose and objective of the research and the things that would be done with the results; it also includes a confidentiality clause wherein the researchers agreed to safeguard their identity and other personal details. Despite securing this, the participants were also informed that they could terminate their participation anytime. During the initial interview and actual sorting, ample time was given for each participant to respond and finish the task at hand. The researchers likewise ensured that a favorable testing condition exists in the room where the data gathering took place.

Data Analysis

The PQ-method software version 2.20 was used to analyze the sorting performed by the 23 participants. Data gathered were subjected to principal component analysis and varimax rotation of factors. Based on these procedures, the distinct factors serve as indicators of the motivation of the participants when they engage in computer hacking. The

Table 1 Major themes of the Q-sample

Themes	Statements
Social-positive	1, 2, 9, 12, 13, 15, 16, 38, 42, 43, 48, 49 *Hacking provides opportunities to socialize*
Social-negative	3, 7, 8, 14, 17, 20, 31, 33, 44, 54 *Hacking is an opportunity to seek attention, get revenge, take advantage of others and show others how superior I am*
Intellectual gain	5, 18, 21, 26, 30, 32, 35, 40, 46, 47, 53, 56 *Hacking provides opportunities for gaining knowledge and development of cognitive skills*
Self-satisfaction	11, 25, 27, 29, 34, 41, 50, 52, 55 *Hacking leads to self-gratification, fulfillment, satisfaction and feelings of accomplishment*
Economic rewards	4, 19, 60 *Hacking is a source of income that can lead to financial stability*
Technological-positive	22, 23, 36, 37, 39, 57, 58, 59 *Hacking is good as it exposes lapses in security that can be rectified and fixed*
Technological-negative	6, 10, 24, 28, 45, 51 *Hacking is the result of knowledge of binary codes and computer languages and can be done regardless if privacy and laws are broken*

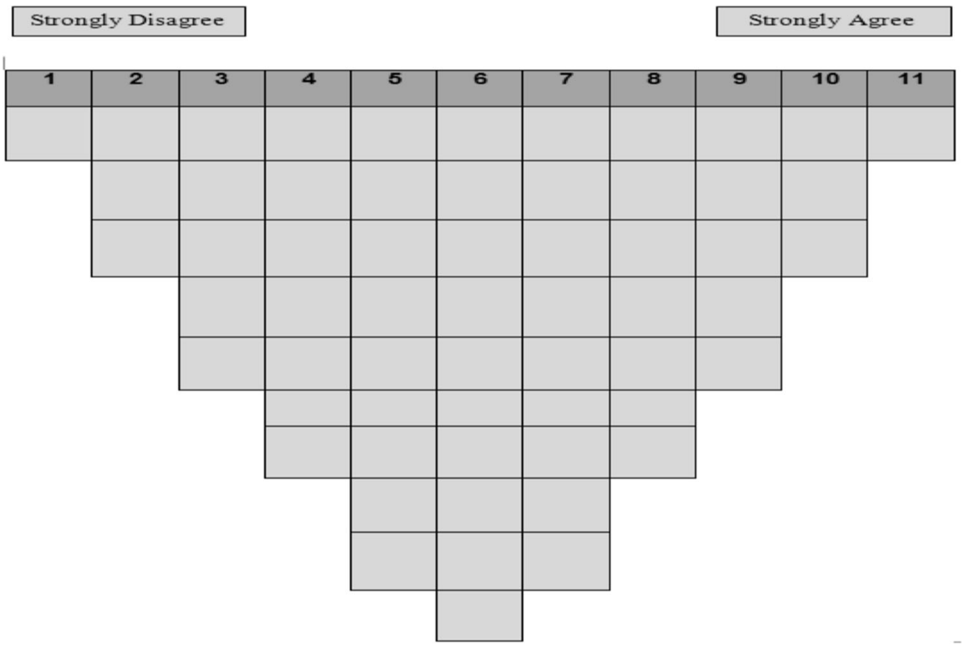

Fig. 2 The Q-sort table

distinct factors are made up of distinguishing Q-samples with the following factor scores: 5, 4, 3, 2, 1, 0, −1, −2, −3, −4 and −5. Distinguishing Q-samples are determined via their corresponding p values ($p < 0.01$).

Results

Review and analysis followed the transcribing of the responses of the participants from the interview phase resulting into 60 statements grouped into seven categories based on their common theme: (1) social positive; (2) social negative; (3) intellectual gain; (4) social satisfaction; (5) economic rewards; (6) technological positive; and (7) technological gain. The social positive category has 12 statements all pertaining to the opportunities to socialize while hacking. A total of ten statements are under the social negative category, and all deal with the psychological needs of hackers to seek attention, get revenge and take advantage of the inferiority of others by demonstrating how superior they are. The intellectual gain category focuses on the belief that hacking provides opportunity for cognitive growth and skills development; it is composed of 12 statements. The self-satisfaction category has nine statements, and all of them revolve around the notion that hacking is a source of self-fulfillment and gratification. A total of three statements were categorized under economic rewards and stress the notion that hacking can bring financial rewards and stability. The technological positive category is made up of eight statements that highlight the positive aspect of hacking as it is an opportunity to identify the weaknesses and flaws of a computer system, while the technological negative category deals with six statements that stress the belief that hacking can be done by those who are knowledgeable regardless of existing regulations and laws.

The corresponding scores obtained after the sorting process were analyzed using the PQ-method software 2.20. The result are three distinct factors highlighting the perception of the respondents regarding the reasons or motivations of Filipino computer hackers. Table 2 contains the composite factor scores for the three identified factors where their corresponding distinguishing statements have been marked.

During the conduct of the analysis, each of the participants was identified to a specific factor via their loading score of 0.36 and above. From the 23 respondents, 11 were loaded to the Factor A (superiority), five for Factor B (exploitative), four for Factor C (opportunistic), while three of the participants did not significantly load to any of the three factors.

In addition to this, the relationship of the factors with each other was also identified as well as their corresponding composite reliability. Result shows that the factors have low to moderate relationship with each other: factors A and B ($r = 0.36$); factors A and C ($r = 0.40$); factors B and C ($r = 0.27$). Nonetheless, all three factors reported high reliability of 0.98, 0.96 and 0.95, respectively.

The merging of the distinguishing statements exclusively per factor and the data from the interview became the basis of the development of the descriptions of each Factor. The descriptions revolve around the perception of the respondents about their motivation when engaged in

Table 2 Composite factor scores of the motivation of computer hackers

Statements	Factor A	Factor B	Factor C
1. I hack because I gain new friends	−4*	0*	−2*
2. I hack because it boosts my self-confidence	−1*	1	2
3. Hacking makes me feel superior among other people	0	−1	2
4. I hack because I earn a lot of money	−2*	3*	−4*
5. Hacking allows me to gain more knowledge	4*	1	2
6. Hacking gives me a sense of authority	0*	−2*	3*
7. Hacking makes me cautious	2	−1*	0
8. I get revenge from hacking	−4	−4	0*
9. I hack to convey my opinion	−2	−4	−3
10. I stalk someone by hacking	−5*	−2	−1
11. Hacking entertains me	−2*	0*	4*
12. I hack because I want to know more about people	−2	−3*	−1
13. I hack in order to help other people	4*	0	−1
14. I hack because I get the attention	−3	−5	0*
15. I can express myself more when hacking	−3	−3	−3
16. I feel happy when I get to help people through hacking	0	−1	−2
17. I hack to take advantage over others	−3	0*	−2
18. I become more conscious because of hacking	1*	−2	−1
19. Hacking is a form of living	−1*	3*	−4*
20. Hacking gives me a sense of pride	−2*	1	3
21. Hacking satisfies my curiosity	2	2	5*
22. I hack because it proves my maturity in technology	1	2	0
23. Hacking gives me a sense of protection	1	1	0
24. I hack because I get free access to products	−1	4*	0
25. I hack because it is fun	1	1	4*
26. I hack because I get access to information otherwise inaccessible	2	3	0*
27. Hacking boosts my self-esteem	0*	2	4
28. It allows me to circumvent certain payments	−2	4*	−2
29. Hacking makes me feel good	−1	0	1
30. Hacking helps me improve my skills constantly	2	2	3
31. Hacking helps me get back to my enemies	−4	−4	−3
32. Hacking facilitates learning	5*	−1*	1*
33. I become competitive because of hacking	0	−1	1
34. Hacking boosts my ego	−3*	0	1
35. Hacking gives me more control over some aspects of my life	−1	−2	−1
36. I hack because I do not have trust in the government	−3	−3	−4
37. I hack to double check security lapses	2	0	1
38. Hacking broadens my connections	−1	2*	−2
39. I hack in order to help retrieve lost information	1	1	1
40. Hacking challenges me	4	0*	3
41. Hacking makes me feel good	−1*	1	2
42. I hack to prove a point	1*	−3	−1
43. I hack to widen influence	0	0	−3*
44. I hack to get other people's attention	−2	−3	−2
45. I hack to manipulate programs	1	5*	1
46. I get to increase my knowledge through hacking	3	3	2
47. I get to widen my experience when I hack	2	0*	3
48. I hack because I care	1*	−2	−3

Table 2 continued

Statements	Factor A	Factor B	Factor C
49. I hack to help others	3*	−1	−2
50. I get to feel a sense of achievement when I hack	1	3	0
51. Hacking is a way to my power in cyberspace	0	−1	−1
52. It gives me a sense of contentment	0	2	1
53. I have the desire to learn more knowledge	3	1	2
54. I hack to impress my acquaintances	−1	−2	0
55. I get mentally and emotionally satisfied	0	1	−1
56. My self-control is practiced through hacking	−1	−2*	0
57. Hacking allows me to eliminate computer viruses	3	−1*	2
58. Hacking allows me to know loopholes in my own network	3	2	−1*
59. To prevent cyber attackers from accessing my files and my system	2	−1	1
60. I hack to be employed	0*	4*	−5*

Factor 1—personal accomplishment; factor 2—exploitation; factor 3—need satisfaction

* Distinguishing statement for a factor ($p < 0.01$)

computer hacking. As previously indicated, the factors revolve around the theme of personal accomplishment, exploitation and need satisfaction.

1. Factor A (superiority): Participants belonging to this factor are motivated by a sense of accomplishment every time they hack into a computer or computer system. Despite the negative connotation that is associated with computer hacking, the participants tend to look at the entire process in a more positive way. For them, hacking can be an opportunity [5] to gain more knowledge so that they can [13] [49] help other people, and because of this, they enjoy a sense of personal fulfillment as they are able to put their skills into good use. Such feelings are characterized by a boost in their [2] self-confidence and [27] self-esteem making them [41] feel good as they are able to demonstrate that they [48] care for others. In addition, their skills and knowledge of hacking [18] have made them more cautious knowing that in a technology-based society, almost everyone is vulnerable. If employed, they hack [42] to prove a point or [10] monitor or stalk a particular individual or organization; the result of which is often the basis of strengthening company protections from other hackers. This sense of achievement is often associated with a [34] boost in ego and a [20] sense of pride.
2. Factor B (exploitative): For these participants, the act of computer hacking has provided opportunities to exploit or take advantage of others. Hacking for them is both [40] a challenge and an opportunity [47] to expand one's experience and [38] broaden connections particularly if one's intention is to be part of a group. Their main purpose for hacking [12] is to get to know others, [17] take advantage of those who are vulnerable, [24] gain free access to many ranges of products and services, [45] manipulate computer programs and [28] circumvent obligations like payments. These practices have taught them to be [7] more cautious and [56] self-controlled and they are often on guard especially for [57] computer viruses that could attack their own system and counter their attacks.
3. Factor C (opportunistic): Those belonging to the group see hacking as an opportunity that could satisfy their immediate needs. Hacking for them is an opportunity to [21] satisfy their curiosity, and they often do it out of [25] fun and to [14] get attention as they will be able to demonstrate their [43] influence. Likewise, the participants under this group see hacking as an opportunity to [26] access the information they need when it is not readily available and also a way to protect themselves [58] by identifying weaknesses in their own network. Finally, when the need arises, they see hacking as a tool [8] for revenge.

Discussion

Following the extraction of the factors using by-person factor analysis, the results summarize the key themes and ideas that describe the motivation of computer hackers. In general, the results bear some resemblance to previous studies that have attempted to document the motivation of computer hackers. Similar to past works, this study found out that computer hackers are also motivated by external rewards like recognition and monetary compensation for every successful hack. This is similar to Gold (2011) where greed was identified as one of the most common motivation of hackers. The respondents also reported that they engaged in hacking activities as a means to express their displeasure or to stress or prove a point which is similar to what Bainbridge (1997) discovered where hacking has been used by employees who were dissatisfied with the management.

The three factors extracted organize the reasons why hackers engage in hacking activities despite it being illegal. Such organization can aid in understanding the dynamics of hacking particularly why these individuals have committed themselves to do an act that has long been considered illegal and a nuisance. The three factors are distinct from each other and focus on the different reasons why hacking takes place. Factor A—superiority—underscores the positive side of hacking, similar to the motivation held by white hats, while those under factors B—exploitative—and C—opportunistic—can be classified as black hats because of their ability and willingness to take advantage and exploit vulnerable people and computer systems and that they engage in hacking activities with no valid or acceptable reason. All motivation identified under the three factors can be anchored on the expectancy-value theory of motivation (Wigfield & Eccless, 2000). The theory underscores the importance of expectations and value in the choices, persistence and actual performance of an individual. This would mean that computer hackers have high expectations and see value in the choices that they make and in the actions that they take. As mentioned earlier, factor A—superiority—highlights the good use of computer hacking. Respondents sorted in this factor experience the general feeling of pride and achievement after every successful hacking attempt. This stems from their expectancy belief that every time they engage in such activity, they will always be successful just like the previous hack. The successful hack leads to an increase in self-confidence level creating a positive impact on their self-concept and efficacy beliefs, as echoed by the expectancy-value theory (Wigfield & Eccless, 2000). Similarly, those sorted in this factor also see high value or usefulness in hacking despite its negative connotation. This view held by the participants influences their persistence and performance as predicted by the expectancy-value theory (Wigfield & Eccless, 2000). According to the respondents, the positive aspects of computer hacking include an opportunity to help others and improve technological skills so that those skills can be used to protect computer systems from black-hat hackers. This is in line with Hoath and Mulhall's (1998) view that not all reasons for hacking are bad or criminal just like those held by black-hat hackers.

Black-hat hackers are those individuals who violate computer security and by so doing often commit illegal acts. Based on the results, the motivation of these individuals is similar to that of factors B—exploitative and C—opportunistic. They view the hacking process as an opportunity to exploit others and the weaknesses of a computer or network system or engage in hacking without any reason. Factor B—exploitative—describes hacking as an opportunity to circumvent the law as it is often used to gain access to information that is deemed secure and not for public use; it has also been used to manipulate computer programs, receive free products and avoid financial obligations, while factor C—opportunistic—describes hackers who engage in such activity out of curiosity or impulse and operate mainly out of wants or desires. They engage in such activity only because of their present circumstances rather than something that is long term like factors A—superiority and B—exploitative. Most respondents who identified themselves under this factor see hacking as an opportunity to be known or famous as they get the attention that they need or require. They often start out of curiosity but continue to engage in such because it is fun and they are able to showcase their computer skills. In applying the expectancy-value theory (Wigfield & Eccless, 2000), factors B—exploitative—and C—opportunistic—highlight a motivation based less on expectancy and more on task value. Hackers under the two factors put emphasis on the utility value of hacking whereby the behavior is more fueled by the external gains it would receive after its execution and the satisfaction of one's curiosity or desire. The respondents appear to have chosen to engage in hacking computer or network systems because of the external rewards that they would be able to get as compared to that of factor A—superiority.

Conclusion

The purpose of this exploratory study was clear; the researchers wanted to explore the motivation of computer hackers by looking at it from a psychological standpoint. They opted to use the Q-methodology approach since it is seen as the most appropriate method of analyzing subjective data like the motivation of computer hackers. Based on the analysis performed, three distinct factors emerged, and the themes exuded by these factors were anchored on the expectancy-value theory of motivation.

The initial results show that in general the motivation of computer hackers operates within the spectrum of expectancies and values where their general motivation stems from the expectations that they will be able to successfully hack their target without getting caught and they continuously perform these acts because of its importance or it is of value to them. In addition, the theme from the three factors extracted revolves around the hackers' desire to demonstrate their capabilities that they can successfully hack a computer system and put the skills into good use (factor A—superiority), to exploit and take advantage of others or systems for external rewards (factor B—exploitative) and to satisfy one's curiosity or to simply demonstrate that they can do it without adhering into any advocacy or ideology (factor C—opportunistic). The three factors or group of hackers very much resemble the common or global categories of white, gray and black hackers which was previously discussed in the introduction of this paper.

The above result contributes to the few literature on the psychological aspect of computer hacking and at the same time provides opportunities to expand research in the field. New qualitative and quantitative researches may be conducted in order to validate the proposed classification. Aside from furthering or expanding the discourse about the motivation of computer hackers, the researchers intend to make use of the proposed classification to develop and standardize a scale that can psychometrically assess and measure motivation of computer hackers. Counseling, clinical and forensic psychologists can make use of the new scale to understand the plight of computer hackers and assess their motivation. Data gathered can serve as a basis for intervention programs particularly designed to manage the behavior of black-hat hackers. The new scale can also be used by future researchers in conducting a large-scale research on the motivation of hackers.

References

Adam, A., & Ofori-Amanfo, J. (2000). Does gender matter in computer ethics? *Ethics and Information Technology, 2*(1), 37–47.

Atkinson, J. W. (1957). Motivational determinants of risk taking behavior. *Psychological Review, 64*(6), 359–372.

Bainbridge, D. (1997). Cannot employees also be hackers? *Computer Law and Security Report, 13*(5), 352–354.

Blatchford, C. (1998). Hacking: Myth or menace. *Computer Fraud & Security, 2,* 16–18. doi:10.1016/S1361-3723(00)87011-6.

Bong, M., & Skaalvik, E. M. (2003). Academic self-concept and self-efficacy: How different are they really? *Educational Psychology Review, 15*(1), 1–40.

Cross, R. M. (2005). Exploring attitudes: The case for Q methodology. *Health Education Research, 20*(2), 206–213.

Dalal, A. S., & Sharma, R. (2007). Peeping into a hacker's mind: Can criminological theories explain hacking? *The ICFAI Journal of Cyber Law, 6*(4), 34–47.

Deci, E. L., Vallerand, R. J., Pelletier, L. G., & Ryan, R. M. (1991). Motivation and education: The self-determination perspective. *Educational Psychologist, 26*(3, 4), 325–346.

Dziopa, F., & Ahern, K. (2011). A systematic literature review of the applications of Q- Technique and its methodology. *Methodology, 7*(2), 39–55.

Eccles, J. (1983). Expectancies, values, and academic behaviors. In J. T. Spence (Ed.), *Achievement and achievement motives: Psychological and sociological approaches* (pp. 75–146). San Francisco, CA: W. H. Freeman.

Eccles, J. S., & Wigfield, A. (2002). Motivational beliefs, values, and goals. *Annual Review of Psychology, 53,* 109–132. doi: 10.1146/annurev.psych.53.100901.135153

Fersizidis, P., Adams, L., Kashdan, T., Plummer, C., Mishra, A., & Ciarrochi, J. (2010). Motivation for and commitment to social values: The roles of age and gender. *Motivation and Emotion, 34*(1), 354–362. doi:10.1007/s11031-010-9187-4.

Gold, S. (2011). Understanding the hacker psyche. *Network Security, 12,* 15–17. doi:10.1016/S1353-4858(11)70130-1.

Gold, S. (2014). Get your head around hacker psychology. *Engineering and Technology, 9*(1), 76–80.

Hoath, P., & Mulhall, T. (1998). Hacking: Motivation and deterrence, part I. *Computer Fraud & Security Bulletin, 4,* 16–19. doi: 10.1016/S1361-3723(97)86611-0

Latham, G. P., & Pinder, C. C. (2005). Work motivation theory and research at the dawn of the twenty-first century. *Annual Review of Psychology, 56,* 485–516. doi:10.1146/annurev.psych.55.090902.142105

Lavrakas, P. J. (Ed.). (2008). *Encyclopedia of survey of research methods* (1st ed.). London: SAGE Publications. doi: 10.4135/9781412963947.

Menkus, B. (1991). USA census data still suspect. *Computer Fraud & Security Bulletin, 8,* 4. doi:10.1016/0142-0496(91)90268-A.

Möjhrenschlager, M. (1995). Hacking: To criminalize or not? Suggestions for the legislature. *Computers & Security, 14*(2), 103–112.

Pruslow, J., & Owl, R. (2012). Demonstrating the application of Q methodology for fieldwork reporting in experiential education. *Journal of Experiential Education, 35*(2), 375–392.

Raje, F. (2007). Using Q methodology to develop more perceptive insights in transport and social inclusion. *Transport Policy, 14*(6), 467–477.

Rogers, M. K. (2002). *A new hacker taxonomy*. Unpublished manuscript, Department of Psychology, University of Manitoba, Winnipeg, Canada.

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation, 3*(2), 97–102.

Rogers, M. K., & Ogloff, J. (2003). Understanding Computer Crime: A comparative analysis of Canadian computer and general criminals. *Canadian Journal of Police & Security Services, 1*(4), 366–376.

van Exel, J., & de Graaf, G. (2005). *Q methodology: A sneak preview*. Unpublished manuscript, Department of Health Policy & Management, Institute for Medical Technology Assessment, Rotterdam, Netherlands and Department of Public Administration & Organization Science, Vrijie Universiteit, Amsterdam, Netherlands.

Wigfield, A. (1994). Expectancy-value theory of achievement motivation: A developmental perspective. *Educational Psychology Review, 6*(1), 49–78.

Wigfield, A., & Cambria, J. (2010). Student's achievement values, goal orientations, and interest: Definitions, development, and relations to achievement outcomes. *Developmental Review, 30,* 1–35. doi:10.1016/j.dr.2009.12.001

Wigfield, A., & Eccless, J. S. (2000). Expectancy-value theory of achievement motivation. *Contemporary Educational Psychology, 25,* 68–81. doi:10.1006/ceps.1999.1015.

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *Howard Journal of Criminal Justice, 44*(4), 387–399.