Copyright © 2017 International Journal of Cyber Criminology – ISSN: 0973-5089
January – June 2017. Vol. 11(1): 78–97. DOI: 10.5281/zenodo.495773
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers

Renushka Madarie[1]
Research and Documentation Centre (WODC), The Netherlands

Abstract

Although much has been written on topic of hacker motivations, little empirical research has been conducted and even less research has attempted to quantify hackers' motivations. The present study analyses relationships between the frequency of several hacking behaviours and motivations to hack in a sample of male hackers and potential hackers. Motivations frequently recurring in the literature are assessed and Schwartz's (1992) Theory of Motivational Types of Values is applied. A preference for self-transcendence and openness to change values was found in the whole sample. Intellectual challenge and curiosity were rated as the most important motivators to circumvent security systems. However, correlation analyses signified the importance of aversion of conservation values. Hackers appear to be more motivated by what they dislike rather than by what they value. Future studies are needed to further examine the discrepancy between hackers' ranking of motivations and the relationship between motivations and hacking behaviours.

Keywords: Hackers, Motivations, Schwartz; Theory of Motivational Types of Values, Hacktivism.

Introduction

The activity of hacking is a contested topic as scientists, practitioners, the general public, and even hackers themselves continuously debate about what "hacking" exactly is and who can be considered a hacker. The definition of hacking has changed over time, as well as its connotation, which in turn influenced the way hackers are perceived. Levy (2010) has extensively investigated the hacker culture, starting with the hackers at the Massachusetts Institute of Technology (MIT) in the fifties and sixties. Initially, the word "hack" was used to describe elaborate college pranks by MIT students that had nothing to do with computers. In the late fifties, the use of this term changed quickly when a few young students became intrigued with the large mainframes at their university. Once they had access to these computers, they worked day and night to explore their possibilities by debugging existing programmes and writing new programmes. By this time, a hack

[1] Research and Documentation Centre (WODC), Ministry of Security and Justice, PO Box 20301, 2500 EH The Hague, The Netherlands. Email: r.madarie@hotmail.com

represented an act involving the computer that demonstrated "innovation, style, and technical virtuosity" (Levy, 2010, p. 10). This pride in hacking was stripped during the eighties when law enforcement, popular press, and private corporations began to criminalise hacking activities and portray hackers as disobedient citizens, or worse: as enemies of the state (Nissenbaum, 2004; Halbert, 1997; Kilger, Stutzman, & Arko, 2004; Taylor, 2005).

Indeed, several hackers did cause great damage to companies and individuals, and consequently to society at large (Nissenbaum, 2004; Australian Institute of Criminology, 2005). However, focusing only on hackers with destructive intents hampers the garnering of insight into hackers' minds. This narrow focus also neglects the fact that hackers form a heterogeneous community (Barber, 2001). The tendency to classify hackers as either 'good' or 'bad' appears to decrease in the literature with the emergence of less judgmental categories, such as hacktivists (hacker activists; Conway, 2003; Woo, Kim, & Dominick, 2009) and script kiddies (novice hackers; Nissenbaum, 2004). More elaborate classifications are based on motivation or intent, but still tend to classify hackers as malicious or non-malicious, since such classifications are often aimed at aiding criminal profiling (Rogers, 2006; Meyers, 2009; Smith & Rupp, 2002).

The few studies that examined the motivations of hackers most often adopted a phenomenological-interpretive approach by interviewing hackers (Jordan & Taylor, 1998; Turgeman-Goldschmidt, 2005; Hutchings, 2013). This approach enables researchers to examine the social and cultural reality from the interviewees' point of view. In other words, hackers are asked to freely express their motivations and the researcher uses their accounts to build a theory (Turgeman-Goldschmidt, 2005). While this type of research certainly has its benefits, the pitfall is that the accounts reported by hackers might be more reflective of culturally recognised motivations than their true personal motivations (Campbell & Kennedy, 2009). Personal motivations can be rather implicit and people might therefore not even be aware of them. The present study examines hackers' motivations by employing an empirically based motivational theory, namely Schwartz's (1992) Theory of Motivational Types of Values.

As previously stated, the hacker community is not homogeneous and hacking is still inconsistently defined. Therefore, in this paper a definition of hacking is employed that captures the diversity of the community and its activities, yet adheres to elements often associated with hacking. These elements are: (1) innovative use of technology, (2) eagerness to explore systems, and (3) programming (The Hacker's Dictionary, 2001; Taylor, 2005; Caelli, Longley, & Shain (1989) in Warren & Leitch, 2010). The definition found in the literature on hacking that best incorporates these elements is put forward by Alleyne (2011, p. 1-2): "an activity which encompasses computer programming, circumventing security systems designed to protect computer networks and digital data stores, designing and executing solutions to solve problems by combining software and hardware in unconventional ways, and modifying and re-purposing digital products of all kinds". Although Alleyne's definition encompasses several (sub)activities, the present paper focuses specifically on hackers who circumvent computer security systems.

The remainder of this paper is structured as follows: First, the Theory of Motivational Types of Values is explained. Subsequently, the studies that quantified hackers' motivations are reviewed and hypotheses are constructed based on this review. Next, the methods and procedures applied are outlined, followed by a description of the results. The

paper concludes with a discussion about the relationship between so-called literature motivations, the motivational types of values, and engagement in hacking activities.

Theory of Motivational Types of Values

Schwartz and Bilsky argued in 1987 that human behaviour is essentially driven by three universal human requirements: biological needs (for organic survival), social interaction (for interpersonal coordination), and social institutional demands (for group survival). These requirements can be translated into values. For instance, a need for group survival might be translated into a strive for world peace. This translation takes place through cognitive development and socialisation processes. The term value here refers to ideals or enduring beliefs about what the world should look like or how people ought to act (Rokeach, 1973; Schwartz & Bilsky, 1990). These beliefs are not situation or state specific and are used as criteria to select and evaluate events, and to evaluate people, including the self (Schwartz & Bilsky, 1978; Schwartz, 1992). Values are thus regarded as criteria, rather than qualities inherent in objects. This view of values implies that they affect behaviour and attitudes (Kristiansen & Hotte, 1996, in Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009), and are therefore motivational drivers.

After extensive testing in more than 20 countries, Schwartz (1992; Bardi & Schwartz, 2003) arrived at a total of ten core motivational types of values. These value types all have two important characteristics: they are each represented by specific items (i.e., the value content), and they are all related to each other (i.e., there is a value structure). The items that form the value content are representations of the corresponding value type. For instance, the value type of power is represented by the items of authority and wealth, and the value type of benevolence is represented by the items of honesty, forgiving, and helpful. In table 1, the ten core motivational types of values are presented along with the corresponding value items. Worldwide research demonstrated that these values are not only recognised in varying cultures, but there also emerged a consistent pattern in the way the value types relate to one another. This pattern forms a continuum of motivational values that Schwartz and Boehnke (2004) structured in a modified quasi-circumplex model. This model visualises to what extent value types are compatible, or in conflict, with other value types. For instance, the model reveals that achievement and power are compatible with each other, while achievement conflicts with benevolence. The modified quasi-circumplex model of value types is illustrated in figure 1.

The influence of these values on everyday behaviour and attitudes has been demonstrated in multiple studies. Schwartz (2013) reports upon three studies that examined the relationship between the motivational types of values and concrete behaviour. First, people who prioritise power values are less likely to show cooperative behaviour than people who prioritise benevolence values. Second, people who highly value self-direction are more inclined to vote for classical liberal parties (emphasizing freedom), whereas people who highly value tradition are more likely to vote for parties that pursue order and control. Third, the higher tradition values are prioritised, the less likely people are to look for contact outside of one's social group. A converse relationship emerged for those who highly prioritise universalism values.

Table 1. Motivational Goals of the Ten Value Types and their Content Items

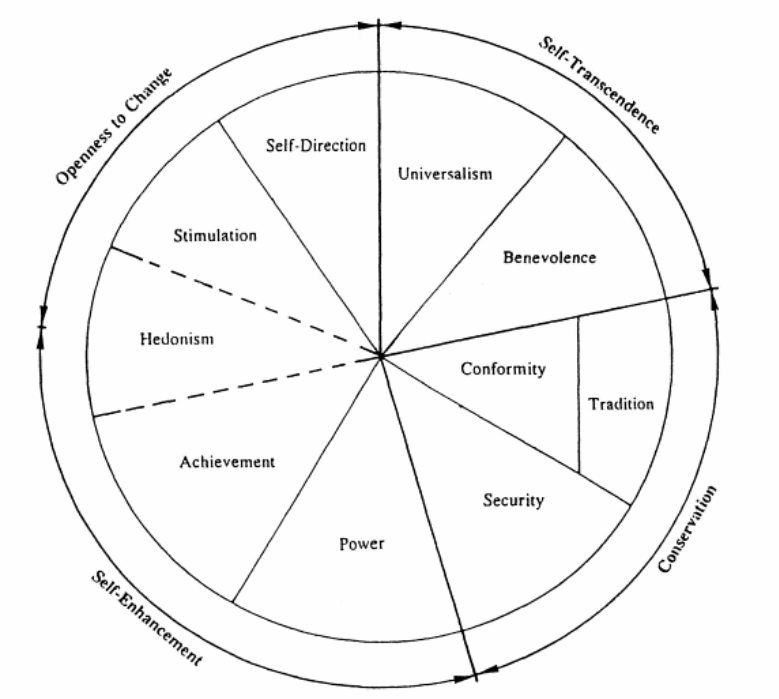
Value type	Value items
Universalism	Tolerance, understanding, appreciation, and protection of people and nature (social justice, equality, peace, wisdom, broadmindedness, protecting the environment, unity with nature, beauty).
Benevolence	Preserving or enhancing the welfare of close others (helpful, forgiving, loyal, honest, responsible).
Conformity	Restraining urges that are likely to harm or upset others, or violate social norms or expectations (self-discipline, politeness, obedience, honouring parents and elders).
Tradition	Respecting, accepting, and committing to customs and ideas imposed on an individual by one's culture or religion (humbleness, moderation, devotion, respect of tradition).
Security	Safety and stability of self, direct relationships, and society at large (national security, family security, social order, reciprocation of favours, clean).
Power	Dominance or control over people and non-human resources, attaining social prestige (authority, wealth, social power and recognition, preserving public image).
Achievement	Personal success or competence as defined by social norms or cultural standards (ambitious, influential, successful, capable).
Hedonism	Pleasure, satisfying sensuous needs (pleasure, enjoying life).
Stimulation	Challenge in life, excitement, and novelty (an exciting life, a varied life, pursuing daring activities).
Self-direction	Autonomy over one's thoughts and actions, not being controlled or influenced by others (creativity, curious, independent, freedom, choosing own goals).

Quantifying Hacker Motivations

Most literature that reports upon hackers' motivations merely explains which motivations can be deduced from the behaviour of hackers and interviews with hackers. Very little research has attempted to determine what motivations are actually important to hackers. The following five studies managed to shed some light on the differential importance attributed to motivations to hack. These five studies serve as the basis for the hypotheses that are tested in the present study.

First, Thycotic Software Ltd (2014) surveyed 127 self-identified hackers live at BlackHat USA. For this survey, 'hackers' were identified as persons who were official attendees of the conference and identified themselves as a hacker. When asked for their primary motivation to hack, 51% stated that they were mostly motivated by fun or thrill-seeking. Approximately 30% chose the option of social consciousness or moral compass, while only 18% chose the option of financial gain. Less than 5% of the hackers were motivated mostly by notoriety.

Figure 1. Modified Quasi-Circumplex Model representing the Structure of Value Types



Adapted from Schwartz (2013).

Second, Woo, Kim, and Dominick (2009) examined the motivations of hackers who defaced web pages by analysing the content of 462 defaced web pages in the English language. Motivations were roughly categorised into two groups. First, 'militant' motivations were confrontational and expressed by reactions against an out-group. More specifically, content was categorised as militant when it hinted at nationalism, ethnicity, religion, freedom of information, and stopping pornography. The latter two motivational causes were observed in 5% of the analysed web pages. Attacks regarding nationalism, religion, and ethnicity were observed in 18% of the analysed web pages. The second group is comprised of 'prankster' motivations. Prankster statements were noted in 71% of the analysed web pages. These statements brag about the hacker's skills (8%), impress a romantic partner (2%), leave a sign (24%; e.g., "hacked by xst", p. 72), or belittle the system administrator (37%).

Third, Goode and Cruise (2006) examined the motivations of 28 software crackers by administering an online survey. The results from this survey demonstrated that the crackers were mostly motivated by stimulation values. 'Personal challenge' was one of the highest rated motivations. At the same time, crackers indicated that they would even crack if they would have to do it anonymously and solitary. Peer recognition, as well as tangible rewards like money, were not considered important drivers. In a similar vein, crackers indicated they were neither motivated by public demand nor by personal need. However, open-ended questions revealed that crackers recognised that they were admired by others,

but greatly differed in their opinion whether gratitude by users of cracked software mattered or not.

Fourth, Fötinger and Ziegler (2004) used data collected with a questionnaire administered by the German Federal Bureau of Criminal Investigation (Bundeskriminalamt, BKA) to analyse the intentions of 599 people who had engaged in identity theft. Personal data related to customers' internet accounts was posted on online forums by perpetrators who actually hacked into the victims computers. This stolen data enabled others to use the internet at the expense of the victims, and thus engage in identity theft. Of the 599 respondents, only six respondents admitted that they had actually engaged in trespassing customers' computers. However, none of these six people stated that they published the account details on the internet. The following results are thus based upon answers from respondents who merely used 'publicly available' stolen details. The two most frequently chosen drivers were: economic reasons (51.3%) and trial and error (33.1%). Amongst the less cited motivations (< 3%) were: fooling around, acceptance of the group, and competition.

Fifth, Turgeman-Goldschmidt (2005) arranged the accounts reported by the 54 hackers he interviewed from the most to the least mentioned. Besides motivations to hack, he also noted factors that might cause people to refrain from hacking and excuses, or justifications, to hack. For the present study, only the reported motivations are taken into account. In descending order, the most reported motivations are: fun, thrill, and excitement, curiosity, computer virtuosity, economic accounts, nosy curiosity and voyeurism, and revenge.

Table 2 presents an overview of the different prioritisations of the reported motivations in the previous five studies. These motivations are structured according to the dimensions of the modified quasi-circumplex model of value types. It can be noted that openness to change value types (i.e., self-direction, stimulation, and hedonism) prevail as primary motivational values for hacking in most studies. The second most noted value types are self-enhancing (i.e., achievement and power). Self-transcendence value types (i.e., benevolence and universalism) are least reported. The lower rating of self-transcendence value types may be due to the fact that hardly any hacktivists were sampled, while these hackers are most likely to be strongly driven by self-transcendence value types. The conservation dimension is not presented in the table since none of the reported motivations could arguably be associated with conservation value types. This absence of conservatism may be due to the inherently progressive nature of computer technology that is the object of hacker activities. The category of 'indeterminate' is added in table 2 to capture motivations that are reported by a large minority of individuals, or even the majority in the study of Fötinger and Ziegler (2004) , but that cannot be readily associated with a value type. For instance, Woo, Kim, and Dominick (2009) assumed that 18% of the web pages they analysed were defaced for nationalistic, ethnic, or religious reasons. However, the underlying motivational values that led to these defacements may differ greatly. For example, on one webpage it was stated: "USA we don't want to be controlled by you", which hints at self-direction values. However, the statement of "USA > ★.CN" could be interpreted as the United States being greater than China, which suggests the importance of power values (Woo, Kim, & Dominick, 2009, p. 72). In a similar vein, hacking for financial gain could result from strive for power or achievement (e.g., Australian Institute of Criminology, 2005; Kshetri, 2006, Turgeman-Goldschmidt, 2005), but Hutchings (2013) rightly discusses the question of whether hacking for money is motivated by need or by greed.

Table 2. Reported Motivations Structured along the Dimensions of the Quasi-Circumplex Value Model

Dimension (value types)	**Thycotic Software Ltd (2004)** *Self-identified hackers (N = 127)*	**Woo, Kim, & Dominick (2009)** *Defaced web pages (N = 462)*	**Goode & Cruise (2006)** *Software crackers (N = 28)*	**Fötinger & Ziegler (2004)** *Identity thieves (N = 599)*	**Turgeman-Goldschmidt (2005)** *Self-identified hackers (N = 54)*
Self-enhancement (power, achievement)	Notoriety (<5%)	Prankster motivations (71%)	Peer recognition (2)	Competition (<3%); Group acceptance (<3%)	Computer virtuosity (3)
Openness to change (hedonism, stimulation, self-direction)	Fun, thrill (51%)		Personal challenge (1)	Fooling around (<3%); Trial and error (33.1%)	Fun, thrill, excitement (1); Curiosity (2); Voyeurism (5)
Self-transcendence (universalism, benevolence)	Social consciousness, moral compass (30%)	Militant motivations (5%)			
Indeterminate	Financial gain (18%)	Militant motivations (18%)		Economic reasons (51.3%)	Economic accounts (4) Revenge (6)

Note. The percentages in parentheses represent the proportion of respondents who rated the motivator as their primary motivator to hack, or the proportion of web pages that was defaced by hackers who were driven by that motivator. The numbers in parentheses represent the relative importance assigned to the motivator compared to the other motivators.

Because the relationship between motivational types of values and hacking activities has not been studied before, it is unclear to what extent the motivations reported in the literature and the motivational values actually relate to one another. Based on the studies that quantified hackers' motivations, it is predicted that the value dimensions and the most often reported motivations in the literature are related in the following way:

- *Hypothesis 1a: self-enhancement value types relate positively to peer recognition and respect.*
- *Hypothesis 1b: openness to change value types relate positively to intellectual challenge and curiosity.*
- *Hypothesis 1c: self-transcendence value types relate positively to justice.*

With regard to the question of what motivational value types prevail in hackers who circumvent computer security systems, it is expected that openness to change value types are the highest rated value types. Furthermore, when self-transcendence value types are highly rated, the hacker is more likely to be engage in hacktivism. Finally, it is expected that conservation value types are the lowest rated values.

- *Hypothesis 2a: hackers who bypass security systems are strongly motivated by openness to change value types.*
- *Hypothesis 2b: hackers who bypass security systems are least motivated by conservation value types.*
- *Hypothesis 2c: hackers who bypass security systems more often engage in hacktivism when they highly value self-transcendence value types.*

Methodology

Participants

Because circumventing computer security systems without consent is an illegal activity, it was not expected that those who engage in this activity would openly talk about it. However, being knowledgeable on computer security is a widely praised skill and often a minimum requirement for engagement in hacking. Therefore, to find hackers who circumvent computer security systems, persons knowledgeable on computer security were asked to participate and subsequently asked if they engaged in hacking. A total of 71 persons agreed to participate. Participants were recruited at the VU University Amsterdam, at computer security conferences, at a hacker workshop, in the personal network of the researcher, and on online public technology forums. Six participants (8.2%) were female. Because few females participated and previous research demonstrated that females differ from males in their value prioritisations (e.g., Schwartz & Rubel, 2005; Ryckman & Houston, 2003), the answers from female participants are excluded from the analyses. The majority of the male participants (56; 86.2%) resided in the Netherlands, eight participants (12.3%) resided in the Czech Republic, and one participant (1.5%) resided in Norway.

Questionnaire

The questionnaire administered to hackers consisted of three parts. The first part inquired about hacking activities. Respondents were asked how often they attempted to circumvent computer security systems on organisations' servers without explicit consent of the organisation, how often they actually circumvented computer security systems on organisations' servers without explicit consent, and how often they engaged in hacktivism. Respondents were asked to provide an answer by ticking one of the following six frequency categories: Never, almost never, once in a while, sometimes, regularly, and often.

The second and third part of the questionnaire inquired about motivations to circumvent security systems. The second part specifically inquired about motivations frequently reported in the literature as primary, or at least important, motivations to circumvent security systems. These motivations are intellectual challenge and curiosity, peer recognition and respect, justice, money, and team-play. Although team-play is

reported relatively little in the literature, several researchers noted that extensive hacker networks exist, both online and offline (Australian Institute of Criminology, 2005; Holt & Kilger, 2012). These networks are not only used for the exchange of knowledge and tools, but also for the formation of hacker teams or groups. To what extent these motivations were motivating to circumvent security systems, or attempt to do this, was rated by respondents on a scale of 1 (not at all) to 5 (very much). These motivations will subsequently be referred to as 'literature motivations'.

The third part of the questionnaire assessed the motivational values of respondents with the 21-item Portrait Value Questionnaire (PVQ; Verkasalo, Lönnqvist, Lipsanen, & Helkama, 2009). The PVQ is composed of 21 scenarios about a person with certain traits, desires, or beliefs. For example, one scenario states: "Tradition is important to him. He tries to follow the customs handed down by his religion or his family." To what extent the person described resembles the respondent was rated on a scale of 1 (not like me at all) to 6 (very much like me). The third part of the questionnaire was used to test hypotheses 2a through 2c.

Procedure

The first two parts of the questionnaire were pilot-tested with nine self-identified hackers at the Dutch security conference Hack in the Box. Based upon their answers, several adjustments were made to the questionnaire. These include increasing the amount of frequency categories to increase the variability in responses, and merging the motivation categories of intellectual challenge and curiosity because they were highly correlated (r_s= .88, $p < .01$). As previously stated, participants were recruited at the university, in the personal network of the researcher, and on online public forums. At the university, a paper version of the questionnaire was handed out. The PVQ scenarios were randomised in two ways, so the influence of neighbour students' answers was minimised. The remainder of the participants filled out an online survey. In the online questionnaire, all scenarios were randomised. At the beginning of each questionnaire, it was stated that participation was completely voluntary and withdrawal from participating was possible at any moment.

Data analyses

A total of 65 questionnaires were analysed. To test the hypotheses, two types of value scales were composed. First, four value dimensions were created by averaging the value items belonging to each of the four value dimensions suggested by Schwartz (1992): Self-transcendence, self-enhancement, openness to change, and conservation. The value dimension of conservation, for example, was composed of the average ratings of the value items belonging to the value types of conformity, tradition, and security. The reliability of these four dimension-scales was measured with Cronbach's alpha, and were respectively: $\alpha_{\text{self-transcendence}} = .66$, $\alpha_{\text{self-enhancement}} = .70$, $\alpha_{\text{openness-to-change}} = .61$, and $\alpha_{\text{conservation}} = .63$. These four dimensions represent the first type of scales. The second type of scales was based upon research that specifically tested the 21-PVQ. Verkasalo and colleagues (2009) constructed two two-dimensional scales with data from over 20 European countries. The scales constructed are (1) the Conservation scale and (2) the Self-transcendence scale. Scores on the Conservation scale indicate the relative importance of conservation value types over openness to change value types. Scores on the Self-transcendence scale indicate the

relative importance of self-transcendence value types over self-enhancement value types. In their paper, Verkasalo and colleagues provide the appropriate value item weights and constants to compute the scale scores.[2] The constants and weights were calculated in a way so that the means of the scales were 100 and the standard deviations 10. The Self-transcendence (ST-SE) scale in the current sample had a mean of 100.41 and a standard deviation of 10.19. However, the Conservation (CO-OC) scale had a mean of 87.67 and a standard deviation of 11.23. As will be elaborated in the results section, the lower mean on the CO-OC scale demonstrates that the participants in the present study scored lower on this scale than the average population where hackers are the minority. The reliability of the CO-OC scale and ST-SE scale are respectively .62 and .54 when estimated with Cronbach's alpha. However, Tarkkonen's General Reliability Coefficient (GRC) is considered a better estimate of the reliability of the scales than Cronbach's alpha (Verkasalo et al., 2009; Tarkkonen & Vehkalahti, 2005). With the GRC, the exact internal consistency is calculated rather than the lower bound. Moreover, the GRC makes less rigid assumptions about equal variances and correlations of the value items. The GRC of the CO-OC and ST-SE scales are respectively .74 and .70.

To test the first hypotheses (1a-c), Spearman's correlation coefficients were computed between the literature motivations, the motivational values, and the four value dimensions. To test the final three hypotheses (2a-c), Spearman's correlation coefficients were also computed for the relationships between hacking activities and motivational types of values. Huismans (in Schwartz, 1992, p. 54) suggested that the relationships between motivational types of values and outside variables are best presented graphically with a sinusoid when the value types are placed on the horizontal axis and ordered according to the circular value structure. A sinusoid is the typical mathematical curve that describes a repetitive oscillation. An example of this curve is provided in figure 2. Schwartz (1992) elaborated that these graphical patterns are more meaningful than the actual significance of the correlation coefficients. Additional logistic regression analyses were conducted to complement conclusions based on the graphical representation of the relationships

[2] In their paper, Verkasalo and colleagues (2009) provide the appropriate value item weights and constants to compute the scale scores. Based upon the reported weights and constants, the following equations were used to compute respondents' scores on the scales:

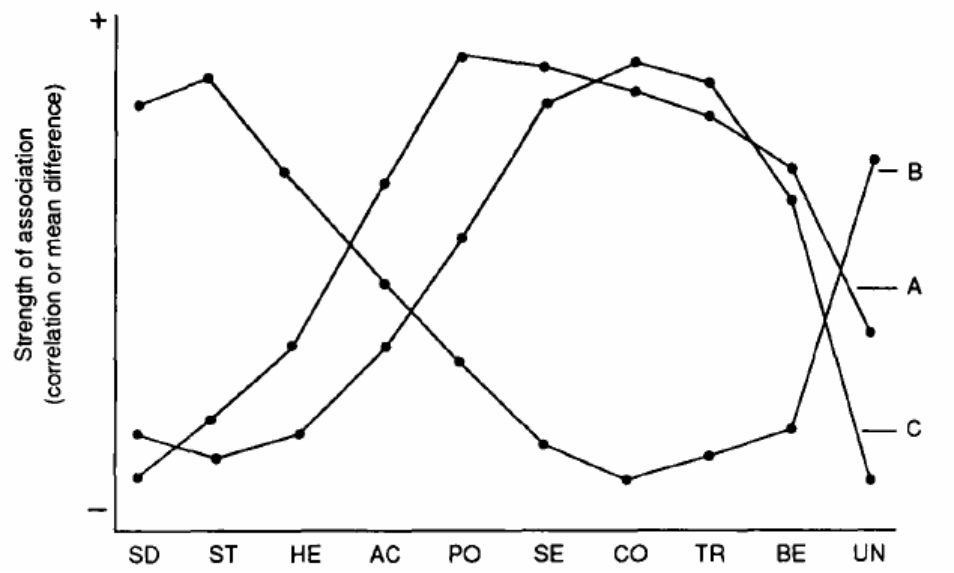
*Conservation (CO-OC) scale: 90.5531 + (-1.1031 * sd1) + (0.5736 * po2) + (-0.3955 * un3) + (0.3430 * ac4) + (1.8516 * se5) + (-1.3589 * st6) + (1.4490 * co7) + (-0.9353 * un8) + (0.8867 * tr9) + (-0.9702 * he10) + (-0.9665 * sd11) + (-0.3883 * be12) + (0.3336 * ac13) + (1.4640 * se14) + (-1.3850 * st15) + (2.3203 * co16) + (1.0024 * po17) + (-0.4133 * be18) + (-0.3065 * un19) + (1.1249 * tr20) + (-0.7511 * he21).*

*Self-transcendence (ST-SE) scale: 67.3577 + (0.4871 * sd1) + (-2.0283 * po2) + (1.6101 * un3) + (-1.5345 * ac4) + (0.0781 * se5) + (0.1803 * st6) + (-0.0952 * co7) + (2.1805 * un8) + (0.8088 * tr9) + (-0.3864 * he10) + (0.6436 * sd11) + (2.2422 * be12) + (-1.8321 * ac13) + (0.2620 * se14) + (-0.8482 * st15) + (0.1396 * co16) + (-1.1128 * po17) + (1.9057 * be18) + (2.1328 * un19) + (0.3330 * tr20) + (-0.3541 * he21).*

Value types are abbreviated: sd = self-direction, po = power, un = universalism, ac = achievement, se = security, st = stimulation, co = conformity, tr = tradition, he = hedonism, be = benevolence. The number after each value type refers to the item in the 21-PVQ.

between motivational values and hacking behaviours. Because (attempts to) circumventing security systems and engagement in hacktivism were significantly non-normally distributed, these variables were dichotomised into two categories: No versus at least once. The logistic regression analyses were conducted with the CO-OC and ST-SE scales, age, and scale use as predictor variables. Schwartz (1992) recommended to account for differences in scale use between groups tested in logistic regressions. Furthermore, Schwartz and Rubel (2005) demonstrated that age affects the importance attributed to motivational types of values. Therefore, preliminary correlations were conducted between age, hacking activities, and motivations to be analysed. Age correlated significantly negatively with conformity (r_s = -.38, p < .01), security (r_s = -.31, p = .02), and the conservation scale (r_s = -.35, p = .01).

Figure 2. Sinusoids Representing Hypothetical Associations between Value Types and Outside Variables



Adapted from Schwartz (1992).

Note. Curves A, B, and C could represent respectively: Age, hours spent gaming, and patriotism. SD = self-direction, ST = stimulation, HE = hedonism, AC = achievement, PO = power, SE = security, CO = conformity, TR = tradition, BE = Benevolence, UN = Universalism.

Results

1. Motivations in the Literature and Motivational Types of Values

The ratings of the value types follow the same structure as the quasi-circumplex model depicted in figure 1. Opposing value types are rated more differently than adjacent value types. For example, universalism and benevolence are rated more similar than universalism and power. The average ratings of the value types are presented in table 3. Schwartz (1992) stated that the different value items of a value type are not per se related to each other. In the present study, the value items that represented one value type were roughly equally rated. A notable exception is tradition. The results of a Wilcoxon signed-rank test

demonstrated that commitment to customs of religion or family (*Mdn* = 2.00) is rated significantly less important than humbleness or moderation (*Mdn* = 4.00; z = -5.78, p < .001, r = -.72).

As for the literature motivations, intellectual challenge/curiosity was rated as the strongest motivator to circumvent security systems (*Mdn* = 5.00, *M* = 4.44, *SD* = 0.90). Peer recognition/respect was the second strongest motivator (*Mdn* = 1.00, *M* = 1.69, *SD* = 0.86). Justice (*Mdn* = 1.00, *M* = 1.56, *SD* = 1.00) and team-play (*Mdn* = 1.00, *M* = 1.51, *SD* = 0.79) were rated as respectively the third and fourth strongest motivator. Money was considered least motivating to (attempt to) circumvent computer security systems (*Mdn* = 1.00, *M* = 1.24, *SD* = 0.77). Because only six respondents considered money as a motivating factor to attempt to circumvent security systems, money will not be analysed in subsequent statistical analyses.

Table 3. Mean Ratings of Motivational Types of Values per Hacking Activity

		M (SD)			
Value Dimensions	Value Types	**Overall (N = 65)**	**Attempt to bypass (n = 55)**	**Bypass security systems (n = 44)**	**Hacktivism (n = 19)**
Self-transcendence	Universalism	4.59 (0.79)	4.59 (0.78)	4.65 (0.78)	4.44 (0.88)
	Benevolence	4.70 (0.94)	4.71 (0.96)	4.67 (0.95)	4.76 (0.98)
Conservation	Conformity	2.82 (1.19)	2.72 (1.17)	2.49 (1.04)	2.37 (0.86)
	Tradition	3.11 (0.85)	3.11 (0.89)	3.11 (0.91)	3.13 (0.98)
	Security	3.30 (1.09)	3.22 (1.06)	3.16 (1.03)	3.26 (1.17)
Self-enhancement	Power	2.95 (0.95)	2.92 (0.95)	3.00 (0.91)	3.23 (0.82)
	Achievement	3.44 (1.11)	3.37 (1.08)	3.36 (1.07)	3.84 (0.82)
Openness to change	Hedonism	4.15 (1.00)	4.16 (1.03)	4.25 (0.98)	4.63 (0.74)
	Stimulation	3.89 (1.29)	3.99 (1.29)	4.14 (1.23)	4.18 (0.97)
	Self-direction	4.88 (0.77)	4.94 (0.75)	5.03 (0.71)	5.08 (0.77)

In the first hypotheses, it was stated that intellectual challenge/curiosity relates positively to openness to change values (1a), justice relates positively to self-transcendence values (1b), and peer recognition/respect relates positively to self-enhancement values (1c). The results demonstrate that intellectual challenge/curiosity indeed positively relates to the openness to change scale (r_s = .30, p = .03), which confirms hypothesis 1a. Justice was not related to any of the self-transcendence value types nor to the self-transcendence scale (r_s = -.00, p = .99), thereby disconfirming hypothesis 1b. In a similar vein, peer recognition/respect was not related to any of the self-enhancement value types nor to the self-enhancement scale (r_s = .13, p = .32). The results therefore disconfirm hypothesis 1c as well. The correlations between the literature motivations and the motivational types of values are presented in table 4.

2. Literature Motivations and Circumventing Security Systems

The results of correlation analyses demonstrate that, although intellectual challenge/curiosity was the strongest motivator, it was not related to the frequency with which respondents circumvent security systems (r_s = -.10, p = .46). The only motivators related to attempts to circumvent security systems and actual circumventing security systems were peer recognition/respect and team-play. The more often a respondent attempted to circumvent security systems, the stronger he was motivated by recognition or respect from peers (r_s = .28, p = .03). The more often a respondent circumvented security systems, the stronger he was motivated by team-play (r_s = .27, p = .05). Positive correlates of the frequency with which one engages in hacktivism are justice (r_s = .37, p < .01) and team-play (r_s = .34, p = .01).

Table 4. Zero-Order Spearman's rho Correlations between Literature Motivations, Value Types, and Hacking Activity

	Literature motivations				**Activity**		
Value types	Intellectual challenge/ curiosity	Peer recognition/ respect	Justice	Team-play	Circumvent security attempts	Cicrumvent security	Hacktivism
UN	.38★★	.03	.02	-.22	-.06	-.09	-.12
BE	.09	.05	.01	.09	-.05	-.16	.04
CO	-.21	-.03	-.15	.04	-.19	-29★	-.24
TR	-.16	.06	.04	-.02	-.16	-.07	.00
SE	-.20	.05	.05	-.10	-.19	-.21	-.07
PO	.12	.17	-.03	.20	.14	.08	.18
AC	.00	.03	.14	.22	-.25★	-.12	.23
HE	.22	-.18	-.18	-.01	-.04	.11	.24★
ST	.09	.08	.07	.07	.12	.19	.15
SD	.42★★	-.03	.02	.04	.06	.14	.14
Self-t	.30★	.05	-.00	-.11	-.07	-.14	-.07
Cons	-.24	.03	-.03	-.04	-.25★	-.28★	-.16
Self-e	.09	.03	.09	.24	-.10	-.08	.28★
Open	.30★	-.04	-.04	.02	.11	.23	.30★

★p< .05, ★★p< .01.

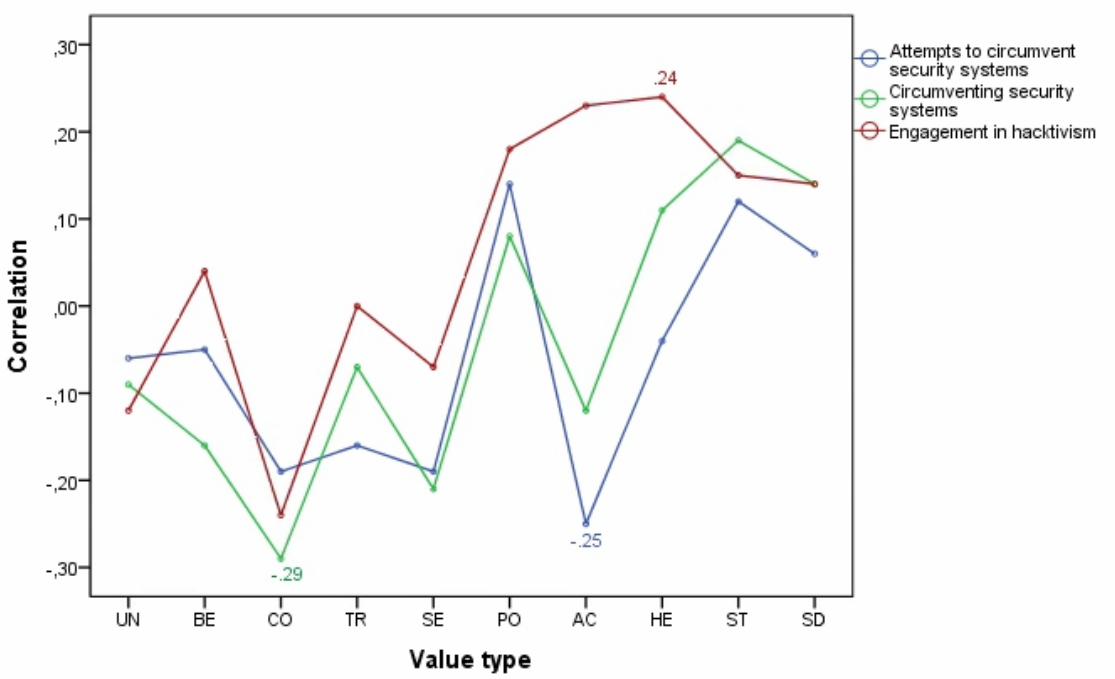
Note. UN = Universalism, BE = Benevolence, CO = conformity, TR = tradition, SE = security, PO = power, AC = achievement, HE = hedonism, ST = stimulation, SD = self-direction. Self-t = Self-transcendence scale, Cons = Conservation scale, Self-e = Self-enhancement scale, Open = Openness to change scale.

3. Motivational Types of Values and Circumventing Security Systems

In the next three hypotheses (2a-c), it was stated which motivational types of values prevail in hackers who circumvent security systems. Figure 3 depicts the correlations between the motivational types of values and the different hacking activities aimed at circumventing security systems. The exact correlations between the motivational types of

values and hacking activities are presented in table 4. In figure 3, the sinusoid pattern of correlation coefficients is least clear for the relationship between attempts to bypass security systems and the motivational types of values.

Figure 3. Zero-Order Correlations between Value Priorities and the Frequency of Hacking Behaviours



Note. Only significant correlations (p< .05) are depicted. Abbreviations of value types are similar to figure 2 and table 4.

The similarity between the three graphs can be explained by the positive relationship between circumventing security systems and hacktivism (r_s = .40, p < .01), and the positive relationship between attempts to circumvent and actual circumventing (r_s = .76, p < .001). In hypothesis 2a and 2b, it was predicted that hackers who circumvent security systems are strongly motivated by openness to change value types (2a) and least motivated by conservation value types (2b). It can be noted in the graphs that openness to change value types are amongst the highest rated value types. Conversely, conservation values are amongst the lowest rated value types. The correlation analyses reveal that the more often respondents circumvent security systems, the less they value conformity (r_s = -.29, p = .02) and the lower their score on the conservation scale (r_s = -.28, p = .03). Furthermore, the openness to change scale was positively related to the frequency with which one engages in hacktivism (r_s = .30, p = .02). These results suggest that hypotheses 2a and 2b are at least partly true. To further test these hypotheses, two logistic regression analyses were conducted. The results of these analyses are presented in tables 5 and 6.

Table 5. Logistic Regression: Value Dimensions as Predictors of Attempts to Circumvent Security Systems on Organisations' Servers

	B (SE)	Wald's χ^2	*p*	Odds ratio
Constant	11.72 (7.55)			
Conservation dimension	-0.10 (0.05)	4.24	.04	0.90
Self-transcendence dimension	0.04 (0.05)	0.80	.37	1.04
Age	-0.06 (0.06)	1.04	.31	0.95
Scale use	-0.81 (1.08)	0.56	.45	0.45

Note. No attempts = 0, attempts = 1. Model χ^2 (4) = 8.53, p = .07, R^2 = .14 (Cox & Snell), .25 (Nagelkerke).

From both table 5 and 6 it can be deducted that respondents who attempted to circumvent security systems as well as actually circumvented security systems are more likely to attribute more importance to openness to change values over conservation values. The odds of attempting to circumvent security systems and actually circumventing security systems for respondents who attributed more importance to openness to change values decreased by 9.5 ($1-e^{-0.10}$) respectively 7.7 ($1-e^{-0.08}$) percent. The results of the logistic regression analyses support hypotheses 2a and 2b as well. Note, however, that the results do not suggest that the respondents simply do not care about conservation values. It could also be that their disdain of conservation values motivates them to (attempt to) circumvent security systems more frequently.

Table 6. Logistic Regression: Value Dimensions as Predictors of Circumventing Security Systems on Organisations' Servers

	B (SE)	Wald's χ^2	*p*	Odds ratio
Constant	6.63 (5.37)			
Conservation dimension	-0.08 (0.03)	6.04	.01	0.92
Self-transcendence dimension	-0.01 (0.03)	0.05	.82	0.99
Age	0.01 (0.04)	0.08	.78	1.01
Scale use	0.48 (0.71)	0.45	.50	1.61

Note. No circumventing = 0, circumventing = 1. Model χ^2 (4) = 8.32, p = .08, R^2 = .13 (Cox & Snell), .18 (Nagelkerke).

In hypothesis 2c, it was stated that hackers who circumvent security systems more often engage in hacktivism when they highly value self-transcendence value types. Figure 3 depicts a rather neutral relationship between the ratings of self-transcendence value types and the frequency with which respondents engage in hacktivism. On the contrary, the self-enhancement scale (r_s = .28, p = .02) and the openness to change scale (r_s = .30, p = .02) were positively related to engagement in hacktivism. The relationship between engagement in hacktivism and the value dimensions was further tested with a logistic regression analysis. To rule out a general lack of interest in hacking, only the 55 respondents who stated that they had attempted to circumvent security systems at least once were entered in this logistic regression. The results of the analysis are summarised in

table 7. Of the respondents who attempted to circumvent security systems at least once, those who assigned more importance to self-transcendence value types were less likely to engage in hacktivism. The odds of engagement in hacktivism for respondents who attributed more importance to self-transcendence values decreased by 14.8 ($1-e^{-0.16}$) percent. Hypothesis 2c is therefore disconfirmed.

Table 7. Logistic Regression: Value Dimensions as Predictors of Engagement in Hacktivism

	B (SE)	Wald's χ^2	*p*	Odds ratio
Constant	8.18 (8.44)			
Conservation dimension	-0.09 (0.05)	3.12	.08	0.92
Self-transcendence dimension	-0.16 (0.07)	5.74	.02	0.85
Age	-1.11 (0.97)	1.30	.25	0.33
Scale use	3.71 (1.71)	4.69	.03	40.89

Note. No hacktivism = 0, hacktivism = 1. Model χ^2 (4) = 15.92, $p < .01$, $R^2 = .33$ (Cox & Snell), .47 (Nagelkerke).

Discussion and Conclusion

This study elaborates upon extant literature on hackers' motivations by empirically determining the importance of several motivators to engage in hacking activities. Both motivators frequently recurring in interviews with hackers and motivational values derived from Schwartz's Theory of Motivational Types of Values are assessed. The results suggest that the relationship between motivators and hacking activities is not as straightforward as may be presumed. Intellectual challenge and curiosity are conceptually related to the openness to change value dimension and rated as the strongest motivators. The more importance is given to openness to change values over conservation values, the more likely it is that people (attempt to) circumvent computer security systems. Intellectual challenge and curiosity, however, are not related to the frequency with which one engages in hacking activities. Because the conservation dimension instead of the openness to change dimension is related to engagement in hacking, it may well be that hackers are rather motivated by what they dislike instead of being motivated by what they value.

The discrepancy between the ratings of the literature motivations and the relationship between these motivations and engagement in hacking supports the idea that the ratings of literature motivations are more reflective of culturally recognised motivations than of true personal motivations. Personal motivations can be rather implicit (Campbell & Kennedy, 2009). People may not be aware of their actual motivations, or do not know how to describe them, because motivations are like 'gut-feelings'. Therefore, when asked for their motivations, it might be that hackers report motivations that they have frequently heard about and subsequently incorporated in their own mental set of representations of these gut-feelings. Schwartz and Bilsky (1987) explain why this process of incorporating terms that reflect motivations occurs. In the following citation, they write about the three universal requirements upon which they based their theory of motivational types of values. However, the same line of reasoning could be applied to gut-feelings of hackers.

> to cope with reality, individuals must recognize, think about, and plan responses to all three [universal] requirements. To be effective members of social groups,

> individuals must communicate about them. Through cognitive development, individuals become able to represent the requirements consciously as goals or values; through socialization, individuals are taught culturally shared terms that enable them to communicate about these goals or values (p. 551).

Socialisation processes could explain why intellectual challenge and curiosity are rated so high, but are not related to the frequency with which one engages in hacking. These motivators are often perceived as relatively innocent motivators (e.g., Goode & Cruise, 2006; Turgeman-Goldschmidt, 2005) and, especially in academic fields, commonly encouraged. Socialisation into the hacker scene is more likely when one engages in hacking more frequently. This could explain why only the social motivators (i.e., peer recognition/respect and team-play) and not the personal motivators (i.e., intellectual challenge/curiosity and justice) are related to the frequency with which one engages in hacking.

Just as not all literature motivations are related to the frequency with which one engages in hacking, so are not all motivational values related to the frequency of engagement. Although the self-transcendence and openness to change value types were considered the most important values in this sample, it were the self-enhancement and conservation value types that actually related to the frequency of engagement. Possibly, the self-transcendence and openness to change value types are expressed by other behaviours than hacking. The average ratings of value types are rather indicative of general personal traits of individuals. These personal traits are subsequently expressed by a variety of behaviours. For example, the tradition item of humbleness and moderation is rated relatively high, whereas the tradition item of commitment to customs of family or religion is rated rather low. The importance attributed to humbleness and moderation has been noted by Fötinger and Ziegler (2004) when describing the hacker community. Humbleness and moderation have little to do with actual hacking behaviour, but more so with interactional behaviour of hackers. Conversely, the low rating of the item of commitment to customs of family or religion is better explained by the progressive nature of computer technology. As opposed to demonstrating humbleness, tinkering with computers is conceptually more related to hacking activities. Indeed, the item of humbleness and moderation is not significantly related to hacking behaviour, while commitment to customs is. A relationship between the other motivational types of values and hacking behaviour may therefore be absent, because only the frequency with which one engages in hacking has been measured.

Limitations and Future Directions

The most important limitations of the present study are sample size and sample selection. Only the rather broad category of hackers who illegally (attempt to) circumvent computer security systems was analysed and no subcategories, other than hacktivists, were distinguished. To find hackers, different channels were consulted and therefore different methods of survey administration were employed which could have differentially affected the results. For example, it is possible that certain types of hackers are less likely to have participated online than offline due to face-to-face contact in the latter setting. However, the use of different channels to find hackers more likely affected the type of hackers that participated than the use of different survey methods did. It would be interesting to

examine in future studies if and how different types of hackers (e.g., script kiddies versus skilled hackers) are motivated by different types of values. Although the present study examined the subcategory of hacktivists, the number of hacktivists is relatively low, which limits the power of the statistical analyses focused on hacktivists. Furthermore, the answers from female respondents were excluded from the dataset because researchers noted that men and women differ in their value prioritisations. For instance, women assign more importance to self-transcendence values and less importance to self-enhancement values than men (e.g., Lindeman & Verkasalo, 2005; Schwartz & Rubel, 2005; Ryckman & Houston, 2003). It is recommended for future studies to include more females in the sample so they can be compared to the male respondents, or to focus specifically on female hackers.

Future studies are needed to assess hacker motivations more empirically and more quantitatively. Qualitative research whereby hackers are interviewed about their motivations did provide some insight into what motivates hackers (e.g., Jordan & Taylor, 1998; Turgeman-Goldschmidt, 2005). However, the results that stem from these interviews are also prone to personal and cultural biases. In quantitative research, more standardised and objective measures can be employed. On a related note, future research could try to establish causal relationships between motivators and hacking behaviour. The present study examined correlations, which do not imply causation. For instance, it is not clear whether people circumvent security systems more often because they value conformity little, or that people who circumvent security systems more often will be more socialised into the hacker community and in turn start valuing conformity less. To conclude, the present study demonstrated a discrepancy between systematically measured motivations and hackers' narratives, and it would be worthwhile to examine the underlying causes of this discrepancy.

Acknowledgement

The author wishes to thank Edward Kleemans for his helpful comments on an earlier draft of this paper.

References

Australian Institute of Criminology. (2005). Hacking motives. *High Tech Crime Brief, 6*, 1-2.

Alleyne, B. (2011). We are all hackers now: Critical sociological reflections on the hacking phenomenon. *Under Review*, 1-32.

Barber, R. (2001). Hackers profiled: Who are they and what are their motivations?. *Computer Fraud & Security*, *2001*(2), 14-17.

Bardi, A., & Schwartz, S. H. (2003). Values and behavior: Strength and structure of relations. *Personality and Social Psychology Bulletin*, *29*(10), 1207-1220. DOI: 10.1177/0146167203254602.

Campbell, Q., & Kennedy, D. M. (2009). The Psychology of Computer Criminals. In S. Bosworth & M. E. Kabay (Eds.), *Computer security handbook*. Hoboken, NJ: John Wiley & Sons.

Conway, M. (2003). Hackers as terrorists? Why it doesn't compute. *Computer Fraud & Security*, *2003*(12), 10-13. DOI: 10.1016/S1361-3723(03)00007-1.

Fötinger, C., & Ziegler, W. (2004). Understanding a hacker's mind - A psychological insight into the hijacking of identities. 1-48.

Goode, S., & Cruise, S. (2006). What motivates software crackers? *Journal of Business Ethics*, *65*(2), 173-201. DOI: 10.1007/s10551-005-4709-9.

Hacker. (2001). In *The Hacker's Dictionary*. Retrieved from http://hackersdictionary.com/html/entry/hacker.html

Halbert, D. (1997). Discourses of danger and the computer Hacker. *The Information Society, 13*(4), 361-374. DOI: 10.1080/019722497129061.

Holt, T. J., & Kilger, M. (2012). Examining willingness to attack critical infrastructure online and offline. *Crime & Delinquency*, *58*(5), 798-822. DOI: 10.1177/0011128712452963.

Hutchings, A. (2013). Hacking and fraud: A qualitative analysis of online offending and victimisation. In K. Jaishankar & N. Ronel (Eds.), *Global criminology: Crime and victimization in a globalized era* (pp. 93-114). Boca Raton: CRC Press.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757-780. DOI: 10.1111/1467-954X.00139.

Kilger, M., Arkin, O., & Stutzman, J. (2004). *The honeynet project: Know your enemy*. Addison-Wesley Professional.

Kshetri, N. (2006). The simple economics of cybercrimes. *Security & Privacy, IEEE*, *4*(1), 33-39. DOI: 10.1109/MSP.2006.27.

Levy, S. (2010). *Hackers: Heroes of the computer revolution*. Sebastopol, CA: O'Reilly.

Lindeman, M. & Verkasalo, M. (2005). Measuring values with the Short Schwartz's Value Survey. *Journal of Personality Assessment, 85*(2), 170-178. DOI: 10.1207/s15327752jpa8502_09.

Meyers, C., Powers, S., & Faissol, D. (2009). Taxonomies of cyber adversaries and attacks: A survey of incidents and approaches. *Lawrence Livermore National Laboratory*, 7, 1-22.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126-139. DOI: 10.1057/ejis.2009.10.

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media & Society*, *6*(2), 195-217. DOI: 10.1177/1461444804041445.

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital investigation*, *3*(2), 97-102. DOI: 10.1016/j.diin.2006.03.001.

Rokeach, M. (1973). *The nature of human values*. New York, NY: The free press.

Ryckman, R. M. & Houston, D. M. (2003). Value priorities in American and British female and male university students. *The Journal of Social Psychology, 143*(1), 127-138. DOI: 10.1080/00224540309598435.

Schwartz, S. H. (1992). Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries. *Advances in Experimental Social Psychology*, *25*(1), 1-65.

Schwartz, S. (2013). Value Priorities and Behavior: Applying. In C. Seligman, J. M. Olson, & M. P. Zanna (Eds.), *The psychology of values: The Ontario symposium* (pp. 1-24). New York, NY: Psychology Press.

Schwartz, S. H., & Bilsky, W. (1987). Toward a universal psychological structure of human values. *Journal of Personality and Social Psychology, 53*(3), 550-562.

Schwartz, S. H., & Bilsky, W. (1990). Toward a theory of the universal content and structure of values: Extensions and cross-cultural replications. *Journal of Personality and Social Psychology*, *58*(5), 878-891. DOI: 10.1037/0022-3514.58.5.878.

Schwartz, S. H., & Boehnke, K. (2004). Evaluating the structure of human values with confirmatory factor analysis. *Journal of Research in Personality*, *38*(3), 230-255. DOI: 10.1016/S0092-6566(03)00069-2.

Schwartz, S. H., & Rubel, T. (2005). Sex differences in value priorities: Cross-cultural and multimethod studies. *Journal of Personality and Social Psychology, 89*(6), 1010-1028. DOI: 10.1037/0022-3514.89.6.1010.

Smith, A. D., & Rupp, W. T. (2002). Issues in cybersecurity: Understanding the potential risks associated with hackers/crackers. *Information Management & Computer Security, 10*(4), 178-183. DOI: 10.1108/09685220210436976.

Taylor, P. A. (2005). From hackers to hacktivists: Speed bumps on the global superhighway?. *New Media & Society*, 7(5), 625-646. DOI: 10.1177/1461444805056009.

Thycotic Software Ltd. (2014). Thycotic Black Hat 2014 Hacker Survey Executive Report.

Turgeman-Goldschmidt, O. (2005). Hackers' accounts hacking as a social entertainment. *Social Science Computer Review*, *23*(1), 8-23. DOI: 10.1177/0894439304271529.

Verkasalo, M., Lönnqvist, J. E., Lipsanen, J., & Helkama, K. (2009). European norms and equations for a two dimensional presentation of values as measured with Schwartz's 21 - item portrait values questionnaire. *European Journal of Social Psychology*, *39*(5), 780-792. DOI: 10.1002/ejsp.580.

Warren, M., & Leitch, S. (2010). Hacker taggers: A new type of hackers. *Information Systems Frontiers*, *12*(4), 425-431. DOI 10.1007/s10796-009-9203-y.

Woo, H., Kim, Y., & Dominick, J. (2004). Hackers: Militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology, 6*(1), 63-82. DOI: 10.1207/s1532785xmep0601_3.