Problems of Forensic Sciences 2013, vol. 93, 391–403

ISSN 1230-7483

THE PERPETRATORS OF COMPUTER CRIMES AS A HETEROGENEOUS GROUP

Jakub LICKIEWICZ

Department of Psychology and Family Studies, Andrzej Frycz Modrzewski University, Kraków, Poland

Abstract

Researchers have often described the hacker subculture as homogeneous. The aim of this study, however, is to identify the differences between groups within this subculture. It distinguishes three groups of hackers: neophytes, who are people new to hacking and have low technical skills, an experienced elite with high technical skills and an utterly inexperienced group known as lamers. The relationship between the psychological and technical factors was evaluated. The NEO-FFI Personality Inventory, the Social Competence Questionnaire and the Test of Internet Addiction were applied to test the thesis. A scale of technical abilities was created with the cooperation of IT experts to evaluate the level of technical skills. Four-hundred-and-twenty-two people participated in the preliminary stage of the research, while 82 were admitted to the second stage. A large number of people were excluded as they were found by the technical questionnaire to lack the required skills. It was only in the second stage that participants were examined using the psychological questionnaires. The research found a relationship between the technical skills and personalities of perpetrators of computer crimes, but uncovered no direct dependence between technical skills, social competence and Internet addiction, which contradicts the stereotypical understanding of hackers.

Key words

Hackers; Computer crime; Personality.

Received 28 August 2012; accepted 4 February 2013

1. Introduction

The high-speed development of information technology has introduced numerous new concepts and phenomena into psychology. The anonymity of the Internet, online aggression and groups created on social-networking sites and services have compelled contemporary psychology to reappraise many theories of human behaviour. This has not eluded forensic psychology, which faces a new challenge in the form of computer crime. The people who commit computer crime are widely known as hackers, however this is a generalisation resulting mainly from the influence of the media. Hacking as a phenomenon had already arisen in the 1950s, while the term itself has gradually come to assume today's pejorative meaning [see 8]. Researchers from a number of disciplines have attempted to explore and explain the particular nature of contemporary computer criminals. Sociologists have attempted to understand the influence of hackers on the way the Internet functions, lawyers have sought ways to penalise crimes committed via the Internet and psychologists have asked questions about the motivation and personality of their perpetrators.

2. Review of research into hackers

The difficulty of gaining access to the hermetic culture of hackers has placed significant limits on research into this population [8]. This review will therefore present only the most representative investigations that have been conducted within the discipline of psychology.

Lieberman conducted a study of 42 hackers using a questionnaire. He found that perpetrators are largely driven by the intellectual challenge, the thirst for knowledge, the desire to know more about computers and the need for achievement and accomplishment. At the same time, he discovered no differences between their level of social anxiety and of avoiding social situations when compared with a group of students. The hackers Lieberman studied had had their first contact with computers at the age of seven. They began programming early and also had problems at school. They did not consider the ethical aspects of what they were doing. The hackers Lieberman studied had a lot of friends and were in heterosexual relationships [7].

Chantler examined 164 hackers and analysed material taken from social networking sites and services, monitoring of the Internet, online questionnaires, e-mails and interviews. He found that the hacker subculture was hierarchical and that hackers often came together in groups of six or seven people, in which each hacker specialised in a different area of programming. To be successful in the hacker community it was necessary to be of at least average intelligence and to be creative, curious and inventive. This very particular group has developed a jargon, which makes it easier to transfer words and emotions using the keyboard (i.e. overcomes the limitations of the keyboard in this respect). All of those studied by Chantler stated that they were addicted to the computer, believed they could do anything they wanted and satisfied their need for power and attainment by hacking into systems. Their targets were mainly military systems, government systems, and university networks [3].

Chantler also attempted to answer the question of why young people begin to hack. He regarded the family environment as a risk factor as the majority of juvenile hackers had been brought up by one parent which often caused them to flee to the computer and lose themselves in it. At the same time, their rejection of the new relationships their single parents embarked upon could lead to a lack of respect for authority also beyond the family. Chantler also took account of such variables as personal details, including when they had begun hacking, home life, education and work experiences, and hacking in his research. Furthermore, Chantler classified the members of the hackers' subculture and assigned them to three groups: an experienced elite, a group of neophyte beginners and a group of utterly inexperienced lamers.

Rogers [11] studied 148 hackers of whom 36 had been convicted and 112 were volunteers. He selected them according to the acts for which they had been committed to a penal institution pursuant to Canadian criminal law. He found the volunteers with the aid of the Internet, where he posted information about his research and a link to his own site on hackers' sites, on pages devoted to computer security and on the website of the American Psychological Association (APA). He used a modified version of Skinner and Fream's questionnaire adapted for the Canadian legal system and for contemporary technical requirements. Those in penal institutions were asked to complete a paper version of the questionnaire, while the volunteers from the Internet filled in an extended computer version which also tested their knowledge of hacking. The aim was also to acquire as much information as possible about the participants. Rogers confirmed a relationship between social learning theory and hacking. He found that this type of crime is heavily dependent on social status, as the equipment and access to the Internet demands material resources. This element may therefore be regarded as a risk factor for hacking. He also observed that the majority of computer crime is committed by young people with an average age of 16, which means that computer skills are acquired at an early age.

In a further set of experiments Rogers et al. [12] analysed the relationship between the personalities of the participants and morality with the aid of the NEO-FFI Personality Inventory. The sample was composed of students of a technical faculty, while the screening test for admission to the group of computer criminals was a questionnaire concerning online behaviour. The questionnaire asked about activities such as password cracking, using someone else's password without permission, looking at other people's files without the agreement of their owner, changing the content of other people's files without their consent, using or writing viruses, acquiring the confidential data of another user without authorisation and the use of special devices to obtain free-of-charge telecommunications services.

All those who declared that they had done some or all of these things were classified as computer criminals. The results of the research revealed that those who committed computer crimes had a higher level of introversion than those in the control group. The remaining hypotheses were not confirmed [12]. Rogers's work resulted in a typology of hackers: newbies (neophytes), cyberpunks looking to gain a reputation, internals breaking into the servers of the companies they worked for, small-time thieves, an old guard embracing first-generation hacker ethics, virus writers, and the experienced (and most dangerous of all professional criminals) cyber terrorists and political activists.

Woo [16] investigated 1,385 people using an Internet questionnaire. Of these, 80% were men and

half were under the age of 19 at the time of the study. Woo found that there was a relationship between an unstable self-esteem manifested in a high level of narcissism and heightened aggression in hackers, who usually react with aggression when under threat. Participants' desire to be at the centre of attention and fantasising about their own powerfulness and greatness were found to be of particular importance. However, as Woo adds, narcissism cannot be treated as proof of high aggressiveness, but only as a risk factor for it. Hackers with higher levels of nationalism displayed more anger in their reactions and behaviour and also had a greater tendency to hack against the sites of states standing opposed to their own nationality. In Woo's opinion, hackers with a high level of nationalism combined with political motivation could cause conflict to spread to the Internet and so increase the risk of cyber terrorism and cybernetic wars. Characteristics such as fantasising about personal greatness, centre of attention, aggressive behaviour, intrinsic motivation, concentration on task at hand and nationalism appeared particularly significant. In Woo's view, these features make it possible to construct a psychological portrait of a hacker engaged in cyber terrorist attacks against other nations. Though these research results are interesting and the majority of the respondents were Koreans, the group was still not homogeneous in terms of nationality. The preferred ways of launching attacks, which could supplement the psychological portraits of perpetrators, were further factors not taken into account.

The Hacker-Taggers group proposed by Warren and Leitch [15] supplements this typology. The members of this group get their pleasure from competing with each other and leave their "calling cards" in the form of a password or symbol on the sites they hack. They usually choose their targets based on current social and political events.

Chiesa, Ducci and Ciappi [4] conducted extensive research on a population of hackers. They employed a questionnaire, in which they asked about demographic data, relations with other people, skills and attitudes to hacking. They also used an adjective scale of their own design that described the personality traits of the participants they surveyed. Their studies encompassed hackers from all over the world, but were mainly based on the personal contacts of one of the project leaders, who has a presence in European hacking circles. Approximately 600 people took part in the project. The investigations began in 2004 and were planned to end in 2012. Other research led by Chiesa, Ducci and Ciappi [12] though interesting, is based exclusively on surveys and does not take into account the cultural aspect: some of the demographic data are inconsistent with the final conclusions, such as in the case of education and hacking or in the case of identifying and defining the power law enforcement institutions have to interfere in the lives of citizens.

The conclusion to be drawn from an analysis of the literature on the subject is that recent and current research into the hacking subculture rests in the main on surveys and questionnaires and does not take account of secondary variables that can often completely change the value of the results. In focusing on motivation they restrict the meaning of the personality factors, which determine hackers' effectiveness and the actions they take. The dominant opinion among the scholars mentioned is that hackers are people with a variety of often mutually exclusive personality traits, who are addicted to the Internet and who have low social competence. This approach means that the majority of the current research, while aspiring to explain the psychological mechanisms of hacking, is in fact closer to sociology. A further problem lies in treating hackers as a homogeneous group, which can also significantly distort the results obtained. The exceptions are the studies done by Chantler [3] and Rogers [12], who propose their own typology of hackers based on the criteria of technical skill and motivation.

3. The research question

As we have seen from the studies presented above, knowledge of information technology (understood in broad terms) and motivation are the factors that distinguish those who commit computer crime. It is assumed for the purposes of this research that a hacker is a person compromising the integrity of a computer system who possesses sufficient skill to gain unauthorised access to it. Yet the perpetrators do not form a homogeneous group. The typology based on the aspect of technological skill should be acknowledged as the most accurate. This is connected with the complexity of an attack and the capacity of hackers to create their own tools. The most important skills that make hackers effective are knowledge of programming languages, of operating systems and of questions involved with network security. This statement shall be taken as the starting point in distinguishing the group of perpetrators. The aim of the research is to answer these questions: Are hackers a heterogeneous group? Do personality traits, social competence and addiction to the Internet distinguish members of the hacker community? If so, what is the nature of these factors? The literature review provides grounds for positing the hypothesis

regarding the heterogeneity of the group and for the possibility of distinguishing at least two sub-classes of distinct hacker skills. It also predicts that there exist statistically significant differences between the groups with regard to personality traits, social competences and Internet addiction.

4. The participants

The participants were people who had committed computer crimes, that is, who had repeatedly gained unauthorised entry to computer systems without the consent of their owners. The participants were chosen with the aid of IT and network security experts who, for the most part, were employed either as network administrators or as police and other officers specialising in computer crime. They put forward the names of people they knew who, in their opinion, possessed high technical skills. Four-hundred-and-twenty-two people participated in the preliminary stage of the research, while 82 were admitted to the second stage. There is a large difference in numbers here because it was necessary to eliminate those who completed the tests in a tendentious manner or who did not meet the main criterion of sufficient technical skill. The results of those who declined to proceed to the second stage of the research were also discarded.

The majority of the participants were men (95%). There were very few women participants (5%). The majority of the respondents gave their age in the intervals 19–24 years (41.5%) and 25–40 years (45%). More than half of the participants had no long-term partner (58.5%), while the remainder either lived with each other (19.5%) or were married (22%). The majority of the participants lived in medium-sized towns (32.9%) and big cities (40.2%), while the remainder lived either in small towns or in the countryside. More than half of the participants had either completed a course of higher education or were in the process of doing so (71.9%).

5. Materials and methods

The study used a questionnaire embracing demographic data and a scale of technical skill covering knowledge of fields such as programming languages, software engineering, databases, operating systems, network issues, graphics applications and other programs to test the hypotheses put forward. The psychological tools deployed were the NEO-FFI Personality Inventory by Costa and McRae [21], Matczak's Social Competence Questionnaire (KKS) [9] and the Test of Internet Addiction (PUI) by Young [10, 19, 20].

The research was conducted in two stages. During the first stage the participants completed an interview posted on a web page, a scale concerning their technical skills and the PUI test. If their level of technical skill met the conditions of the research, they were invited to participate in the second stage, in which they completed the NEO-FFI and KKS questionnaires in paper form. Rogers [11], who looked for volunteers using the Internet and also used it to determine the knowledge levels of participants, adopted a similar research procedure. The interview and the other tests were anonymous and voluntary. The participants were informed of this at the very beginning of the research. The participants also had the right to decline to take part in the second stage of the procedure.

6. Results

Two groups that were different from each other in terms of technical skills were distinguished using k-means cluster analysis. The first sub-group contained 49 participants with low technical skills and the second 33 participants with greater knowledge of programming languages, operating systems and system security. The results obtained confirmed earlier research which indicated that there were fewer people with high technical skills when compared with those of little technical skill [3]. With reference to the literature, the first group was named as the neophytes and the second as the elite. The greatest inter-group differences were observed in knowledge of programming languages, operating systems and network issues. Participants from the elite group have greater skill levels in these areas. The members of the elite group were very much better at programming and more proficient in handling operating systems and the intricacies of the network – including network security methods. The differences are less pronounced with regard to the remaining skills, but the knowledge of the elite is greater than that of the neophytes in all categories.

The second question was the relationship between technical skill and personality and between social competence and addiction to the Internet. The results are presented in Tables I and II below.

As the inter-group comparisons revealed, there are statistically significant differences with regard to neuroticism, openness to experiences and conscientiousness. Participants in the elite group are less neurotic than the neophytes and have greater levels of openness to experience and of conscientiousness. No significant

TABLE I. STUDENT'S t-TEST FOR PERSONALITY TRAITS IN THE ELITE AND NEOPHYTE GROUPS

	Neophytes		Elite				
	M	*SD*	*M*	*SD*	*f*	*t*	*P*
Neuroticism	20.1	8.55	15.42	8.72	0.146	2.409	0.01
Extroversion	26.42	6.04	25.78	6.22	0.064	0.462	n.i.
Openness to experiences	26.89	5.03	30.45	6.11	0.965	–2.767	0.05
Amicability	27.28	4.92	26.06	7.59	5.310	0.887	n.i.
Conscientiousness	28.32	6.75	32.36	7.12	0.270	–2.570	0.01

TABLE II. THE U MANN-WHITNEY TESTS FOR SOCIAL COMPETENCE AND INTERNET ADDICTION IN THE ELITE AND NEOPHYTE GROUPS

	Addiction to the Internet	Intimate contacts (e.g. long-term partner, married, single)	Social contact	Assertiveness	Overall result
U Mann-Whitney	776.000	765.000	720.000	773.000	796.000
Z	–0.32	–0.41	–0.84	–0.34	–0.12
Asymptotic significance (two-sided)	n.i.	n.i.	n.i.	n.i.	n.i.

statistical differences were found between the groups with regard to social competence and addiction to the Internet.

7. Discussion

It was posited that hackers are not a homogeneous population and that the criterion that differentiates them is technical skill. This was completely confirmed as two groups were indicated: participants with higher and lower skill levels. The research did not include people who break into telephone networks or those who create viruses because, with regard to the current level of IT technology development, they were regarded as an insufficiently representative group compared to the population as a whole. The number of people assigned to the individual groups (which were determined by statistical analyses) remained in accord with earlier research into this population, which indicates the small number of people with high technical skills compared to those with average knowledge of IT technology [see 3, 4].

The typology proposed by Chantler [3] is the one that is most consistent with the results obtained. This was the typology used in naming the first group as neophytes and the second as the elite. It was assumed here that the third group identified by Chantler, lamers, were those who did not qualify for the research. They were rejected in the first stage as their technical skills were too low or because they were inclined to overstate their abilities. We may also refer the level of technical skill to Chiesa's typology [4], which classifies hackers as those taking advantage of known loopholes in systems, hobbyists and users of local networks. When comparing this to the results obtained, it can be said that the participants belonged to the first two groups according to Chiesa's typology. That is, those with sufficient skill to carry out attacks based on disseminated system errors or flaws (neophytes) and the elite, who are capable of creating their own tools, whose attacks are more varied and for whom hacking is their long-term passion.

The two groups differ with regard to knowledge of programming languages, operating systems and the principals by which the network functions. It was in these three categories that the greatest disproportions were found. The typology devised by Rogers [11, 12] confirms the thesis adopted, yet covers wider questions also connected with motivation. Marking out the two groups also points to the fact that it is not only the technical evolution of the Internet that is at issue, but also the changes that have taken place in the population of hackers, which is a group that operates in a very specific way and one that we may tend to regard as monolithic. In the first period of their history hackers were treated as a homogeneous group, while the present level of development of IT technology means that they can be divided into those with more and less advanced skills, which affects the way

they behave on the network. It is of course possible for those in the lower group to gain "promotion", but in Chantler's opinion [3] this happens in only a few cases. To move out of the group of neophytes and into the elite it is necessary for hackers to continually seek new challenges and broaden their knowledge. Openness to experience is the decisive character trait in this respect. As new skills are acquired so new tasks and challenges are sought, which leads to a continuous increase in interest in issues and knowledge concerning hacking. This is what is required to be admitted to the elite group [18]. Chiesa, Ducci and Ciappi [4] also refer to the need to raise one's status in the hierarchy. This was precisely the reason for hacking chosen by respondents from among the possible motivations.

The groups differ with regard to technical skills. This was a selection criterion, though the divergence in terms of proficiency in programming languages, operating systems and questions concerning the world wide web was decidedly higher in the case of the elite. This group also has greater knowledge of databases and graphics programs. This means that the high skills levels of the elite do not only involve questions strictly connected with hacking, but also with software as broadly understood. This points to the fact that the generalised knowledge of IT represented by familiarity with programming languages and operating systems also leads to effectiveness and skill in IT as broadly understood.

This relationship is also explained by the earlier discussion concerning the mastering of certain programs based on cooperating with other people. It is necessary to point out here that this relationship appears exclusively in the neophyte group, which suggests that contact with other hackers (perhaps in a search for a sort of mentor) and having recourse to their knowledge and experience is one of the essential elements in their technical development. This, however, would require them to have high self-esteem and an internal locus of control which, according to Chantler [3], result from considerable technical skill. This is also confirmed by Chiesa, Ducci and Ciappi [4], who observed that in a proportion of their participants there was a desire to become a sort of guardian for those with less experience. They add that the first achievements come as a result of the beginner's own experiences of trial and error, yet to acquire more advanced knowledge the assistance of more technically accomplished hackers is needed. For this reason the neophytes attempt to make these sorts of contacts so that they can discuss their experiences as beginners with more experienced hackers.

The second research question posited a difference between the groups under examination with regard to personality traits, social competence and addiction to the Internet. This was partially confirmed as the groups differed with regard to personality traits. However, no statistically significant results were recorded regarding social competence and addiction to the Internet. The elite group was characterised by a lower level of neuroticism and greater openness to experience and conscientiousness. With reference to the literature this makes it possible to draw conclusions concerning the way these people function in the network. Those with higher levels of neuroticism will display more behaviour directed at preserving anonymity on the Internet which, however, when allied with low levels of technical skill, will not always be effective. They may also create more Internet identities and even pass themselves off as other users [2]. At the same time, they will make too much use of CMC (computer mediated communication) and value it more than communication that is not mediated by the Internet. They will be oversensitive and impulsive in their actions, which may mean they will make errors and therefore be more easily apprehended by law enforcement bodies.

Effectiveness and high levels of technical skill may be achieved by those with a high level of cognitive curiosity who are also emotionally balanced, organised and persistent. The key trait is openness to experience and especially one of its elements – tolerance of the new [5]. The effectiveness of hacking activities depends on continuous broadening of knowledge and on the capacity to swiftly adopt new technologies and methods of action. Similar conclusions appear in the research conducted by Chantler [3], who found a higher level of creativity in those belonging to the elite group. The success of the members of this group is also associated with their internal locus of control. A similar position is expressed by Voiskounsky, Babeva and Smyslova [17] who described the members of a group they researched as intellectually curious, astute and quick learners. These conclusions are again supported by Chiesa, Ducci and Ciappi [4], who described the members of a group they researched as creative, clever and, at the same time, as dreamers and rebels. The way hackers describe themselves – as inquisitive, and on the one hand lazy but on the other engaged and committed – leads to similar conclusions. It is likely that this dualism constitutes a criterion distinguishing the groups [4]. There is no doubt that openness to experience is a key trait for the effectiveness of a hacker. At the same time, successful hacking requires competence and a drive for perfection, as well as circumspection and restraint in acting [5]. Those with higher

levels of technical skill plan their actions carefully, are cautious and therefore make very few mistakes. They are therefore able to be very patient when searching for loopholes in the system they are trying to hack. Chantler [3] was correct when he stated that the key to success in hacking was to combine creativity with tenacity. According to Costa and McRae [5] those hackers who are conscientious are those who at the same time observe moral principles scrupulously.

It is also possible to advance the hypothesis that traits opposite to those possessed by the elite group and therefore anxiety regarding interpersonal relationships, lack of drive to improve their skills and a sort of negligent disorganisation are characteristics of those in the lamer groups, who use other people's programs to wreak maximum havoc with the computer systems of their victims.

No divergence in social competence was found in the participants studied, which means that this is not a factor that distinguishes the groups. It is nevertheless necessary to accept the premise that – in connection with the results of other research – there are differences in the way the members of the two groups use the Internet. A higher level of neuroticism was associated with less frequent use of news services [1] and the use of the Internet for entertainment [13]. This also means that both groups may use social engineering as a way of acquiring the data that is important to them. It should however be stressed that because they have an average level of social competence, this will not be their main method of hacking.

The results obtained provided grounds for distinguishing two groups: neophytes and the elite. Their personality traits are consistent with those set out in the current and recent literature on the subject. As the research conducted has shown, perpetrators of computer crime are different not only on account of technical skill but also owing to personality traits and, as Donato suggests, this permits conclusions to be drawn about the way they behave on the Internet, the targets they choose, the methods they apply and even about the effectiveness of their attacks [6]. It may be the case that this knowledge can provide a platform for creating psychological profiles of unknown perpetrators of computer crime that will make it possible to narrow the search for them – especially in situations where they are attacking from within a network.

References

1. Amichai-Hamburger Y., Wainapel G., Fox S., On the Internet no one knows I'm an introvert. Extroversion, neuroticism, and Internet interaction, *CyberPsychology & Behavior* 2002, 5, 125–128.
2. Caspi A., Gorsky P., Online deception: prevalence, motivation, emotion, *CyberPsychology & Behavior* 2006, 9, 54–59.
3. Chantler N., Risk: The profile of computer hacker, University of Technology, Pertch Curtin 1996.
4. Chiesa R., Ducci S., Ciappi S., Profiling hackers. The science of criminal profiling as applied to the world of hacking, CRC Press, New York 2009.
5. Costa R., McCrae P., Osobowość dorosłego człowieka, Wydawnictwo WAM, Kraków 2005.
6. Donato L., An introduction to how criminal profiling could be used as a support for computer hacking investigation, *Journal of Digital Forensic Practice* 2009, 2, 183–195.
7. Lieberman B., Computer hackers. An intractable problem and what to do about it, Pittsburgh 2003 [research and Policy memorandum 301.1].
8. Kirwan G., Power A., The psychology of cybercrime, IGI Global, Hershey 2011.
9. Matczak A., Kwestionariusz Kompetencji Społecznych, Pracownia Testów Psychologicznych PTP, Warszawa 2001.
10. Poprawa R., Dulewicz D., Stress, the sense of coherence and problematic Internet use, [in:] Psychopathologies of modern society. Innocence in danger, Mesjasz J. [ed.], Wydawnictwo WSHE, Łódź 2006.
11. Rogers M., A social learning theory and moral disengagement analysis of criminal computer behavior: en exploratory study, University of Manitoba, Department of Psychology, Winnipeg 2001 [Ph.D. dissertation].
12. Rogers M., A two dimensional circumflex approach to the development of a hacker taxonomy, *Digital Investigation* 2006, 3, 97–102.
13. Shaw L., Gant L., Users divided? Exploring the gender gap in Internet use, *CyberPsychology & Behavior* 2002, 5, 517–527.
14. Turgeman-Goldschimdt O., Hackers accounts: Hacking as a social entertainment, S*ocial Science Computer Review* 2005, 23, 8–23.
15. Warren M., Leitch S., Hackers taggers: A new type of hackers, *Information Systems Frontiers* 2010, 12, 425–431.
16. Woo H. J., The hacker mentality, exploring the relationship between psychological variables and hacking activities, University of Georgia, Athens 2003 [Ph.D. dissertation].

17. Voiskounsky A. E., Babaeva J. D., Smyslova O. V., Attitudes toward computer hacking in Russia, [in:] Cybercrime law enforcement. Security, and surveillance in the information era, Thomas D., Brian D. L. [eds.], Routledge, London 2000.
18. Voiskounsky A. E.. Smyslova O. V., Flow-based model of computer hackers motivation, *CyberPsychology & Behavior* 2003, 6, 171–180.
19. Young K. S., Caught in the net: how to recognize the signs of Internet addiction – and a winning strategy for recovery, John Wiley and Sons, New York 1998.
20. Young K. S., Internet addiction: A new clinical phenomenon and its consequences, *American Behavioral Scientist* 2004, 48, 402–415.
21. Zawadzki B., Strelau J., Szczepanik P. [et al.], Inwentarz osobowości NEO-FFI Costy i McCrae. Adaptacja polska, Pracownia Testów Psychologicznych PTP, Warszawa 1998.

Corresponding author
Dr Jakub Lickiewicz
Krakowska Akademia im. Andrzeja Frycza-Modrzewskiego
Wydział Nauk Humanistycznych i Psychologii
ul. Gustawa Herlinga-Grudzińskiego 1
PL 30-705 Kraków
e-mail: jlickiewicz@afm.edu.pl

Problems of Forensic Sciences 2013, vol. 93, 391–403

SPRAWCY PRZESTĘPSTW KOMPUTEROWYCH JAKO GRUPA HETEROGENICZNA

1. Wprowadzenie

Gwałtowny rozwój technologii informacyjnej wprowadził do psychologii wiele nowych pojęć i zjawisk. Anonimowość Internetu, sieciowa agresja czy też grupy tworzone za pośrednictwem portali społecznościowych zmusiły współczesną psychologię do weryfikacji wielu teorii dotyczących zachowania człowieka. Zjawisko to nie ominęło też psychologii sądowej, która stanęła przed nowym wyzwaniem w postaci przestępczości komputerowej. Popełniające je osoby nazywa się powszechnie hakerami, jakkolwiek stanowi to generalizację wynikającą głównie z wpływu mediów. Samo zjawisko hakingu powstało już w latach 50. XX wieku i stopniowo ewoluowało do dzisiejszego, pejoratywnego znaczenia [por. 8]. Badacze wywodzący się z różnych gałęzi nauk próbują zgłębić specyfikę współczesnych przestępców komputerowych. Socjologowie poszukują wpływu hakerów na funkcjonowanie Internetu, prawnicy sposobu na penalizację przestępstw dokonywanych za pośrednictwem sieci, a psychologowie zadają pytanie o motywację i osobowość sprawców.

2. Przegląd badań dotyczących hakerów

Trudność dostępu oraz hermetyczność kultury hakerskiej powoduje, że badania tej populacji są w znacznym stopniu ograniczone [8]. Z tego względu zaprezentowano wyłącznie najbardziej reprezentatywne z badań z kręgu psychologii.

Lieberman przebadał ankietowo 42 hakerów. Stwierdził, że sprawcy w swoim działaniu kierują się głównie wyzwaniem intelektualnym oraz pragnieniem wiedzy, poznawania komputerów oraz potrzebą osiągnięć. Równocześnie nie wykazał żadnych różnic w poziomie lęku społecznego i unikania sytuacji społecznych w porównaniu ze studentami. Badani przez niego hakerzy pierwszy kontakt z komputerami mieli w wieku siedmiu lat. Wcześnie zaczęli programować, mieli też problemy w szkole. Hakując, nie zastanawiają się nad etycznymi aspektami swojej działalności. Posiadają wielu przyjaciół i utrzymują heteroseksualne związki [7].

Chantler przebadał 164 hakerów, analizując materiał uzyskany z serwisów komputerowych, obserwacji sieci, kwestionariuszy on-line, e-maili oraz wywiadów. Stwierdził, że subkulturę hakerską cechuje system hierarchiczny, często łączą się oni w grupy liczące 6–7 osób, w których każdy specjalizuje się w innej dziedzinie programowania. Równocześnie, aby odnosić sukcesy w tej społeczności, trzeba mieć przynajmniej przeciętną inteligencję, być twórczym, dociekliwym i pomysłowym. Ta specyficzna grupa posiada własny żargon, który ułatwia przekaz słów i emocji poprzez klawiaturę. Wszyscy badani przez Chantlera stwierdzali, że są uzależnieni od komputera, wierzyli, że mogą zrobić wszystko, co zechcą i zaspokajali potrzebę władzy oraz osiągnięć poprzez hakowanie systemów. Ich celem były głównie systemy wojskowe, rządowe oraz sieci uniwersyteckie [3].

Chantler starał się także znaleźć odpowiedź na pytanie, dlaczego młodzi ludzie zaczynają hakować. Za czynnik ryzyka uznał środowisko rodzinne, gdyż większość młodocianych hakerów była wychowywana tylko przez jednego rodzica, co powodowało często ich „ucieczkę w komputer". Równocześnie brak akceptacji nowego związku rodzica mógł skutkować brakiem szacunku dla autorytetów w szerszym tego słowa znaczeniu. W swoich badaniach Chantler uwzględnił takie zmienne, jak dane osobowe, początek działań, życie rodzinne, edukację, doświadczenie, pracę oraz hakowanie. Chantler sklasyfikował także członków subkultury hakerskiej, wyróżniając doświadczoną elitę, początkujących neofitów oraz niedoświadczonych lamerów.

Rogers [11] przebadał 148 hakerów – 36 skazanych i 112 ochotników. Dobierając ich, kierował się czynami, za które zostali osadzeni w zakładzie karnym według kodeksu karnego Kanady. Ochotników dobierał przy pomocy Internetu, zostawiając informacje o badaniach na stronach hakerskich, witrynach dotyczących zabezpieczeń oraz na stronie Amerykańskiego Towarzystwa Psychologicznego (APA) z odnośnikiem na jego stronę. W badaniach użył zmodyfikowanego kwestionariusza autorstwa Skinnera i Freama dostosowanego do kanadyjskiego systemu prawnego oraz współczesnych realiów technicznych. Osadzonych badano kwestionariuszem w wersji papierowej, ochotników z Internetu jego dłuższą komputerową wersją, która sprawdzała także ich wiedzę na temat hakowania. Celem było również uzyskanie jak największej liczby informacji o osobach badanych. Rogers potwierdził związek pomiędzy teorią społecznego uczenia się a hakowaniem. Jego badania wskazują, że ten typ przestępstw zależy w dużym stopniu od statusu społecznego, gdyż sprzęt oraz dostęp do Internetu wymaga zasobów materialnych, dlatego ten element może być uznany za czynnik ryzyka hakowania. Zauważył również, że przestępstwa komputerowe są domeną ludzi młodych, mających średnio 16 lat, co wiąże z wcześnie nabytymi zdolnościami obsługi komputera.

W kolejnych badaniach Rogers [12] analizował zależność pomiędzy osobowością badaną przy pomocy kwe-

stionariusza osobowości NEO-FFI a moralnością. Próbę stanowili studenci wydziału technicznego, a testem kwalifikującym do grupy przestępców komputerowych był kwestionariusz zachowań sieciowych. Dotyczył on aktywności takich, jak: odgadywanie haseł, używanie cudzego hasła bez pozwolenia posiadacza, przeglądanie cudzych plików bez zgody właściciela, zmianę zawartości plików innych osób bez ich zgody, używanie lub pisanie wirusów, uzyskanie poufnych danych innego użytkownika bez jego zgody oraz używanie specjalnych urządzeń w celu uzyskania darmowych połączeń telefonicznych.

Wszyscy, którzy zadeklarowali tego typu działalność, byli klasyfikowani jako przestępcy komputerowi. Wyniki badań wskazały, że osoby popełniające przestępstwa komputerowe posiadają większy poziom introwersji niż osoby z grupy kontrolnej. Pozostałe hipotezy nie znalazły potwierdzenia [12]. Efektem pracy Rogersa była typologia hakerów, w której opisał on nowicjuszy, poszukujących rozgłosu cyberpunków, włamujących się na serwery własnej firmy wewnętrznych, drobnych złodziei, kierującą się etyką hakerską starą gwardię, autorów wirusów oraz doświadczonych i najgroźniejszych z wszystkich profesjonalnych kryminalistów – informatycznych wojowników oraz aktywistów politycznych.

Woo [16] przebadał kwestionariuszem internetowym 1385 osób, z czego 80% to mężczyźni, a połowa nie osiągnęła w chwili badania 19. roku życia. Stwierdził, że istnieje związek między niestabilną samooceną objawiającą się wysokim poziomem narcyzmu a większą agresywnością u hakerów, którą zwykle reagują w sytuacjach zagrożenia. Szczególne znaczenie miała potrzeba bycia w centrum uwagi oraz fantazjowanie na temat własnej wielkości. Jednak, jak dodaje Woo, nie można traktować narcyzmu jako dowodu świadczącego o wysokiej agresywności, lecz jedynie jako czynnik ryzyka. Hakerzy z wyższym poziomem nacjonalizmu przejawiali większą złość w reakcjach i zachowaniu, mieli też większą tendencję do hakowania stron innych państw będących w opozycji do ich narodowości. Zdaniem Woo, wysoki poziom nacjonalizmu u hakerów w połączeniu z motywacją polityczną może spowodować przeniesienie się konfliktów do Internetu i zwiększa w jego opinii ryzyko cyberterroryzmu i cybernetycznych wojen. Szczególnie istotne wydają się takie cechy, jak fantazjowanie na temat własnej wielkości, doświadczenia skoncentrowane na sobie, agresywne zachowania, motywacja zewnętrzna, koncentracja na zadaniu i nacjonalizm. Według Woo, te cechy dają możliwość stworzenia portretu psychologicznego hakera zaangażowanego w ataki cyberterrorystyczne przeciwko innym nacjom. Mimo iż wyniki badań są interesujące, a większość respondentów stanowili Koreańczycy, grupa była niejednorodna pod względem narodowości. Nie uwzględniono też preferowanych sposobów ataków, które mogłyby stanowić uzupełnienie portretu psychologicznego sprawcy.

Swego rodzaju uzupełnieniem tej typologii jest zaproponowana przez Warrena i Leitch [15] grupa hakerów – taggerów, którzy czerpią przyjemność ze współzawodnictwa oraz oznaczania stron internetowych swoim hasłem lub symbolem. Cele wybierają najczęściej w oparciu o aktualne wydarzenia polityczne i społeczne.

Obszerne badania nad populacją hakerów zaproponowali Chiesa, Ducci i Ciappi [4]. Zastosowali oni kwestionariusz, w którym pytali o dane demograficzne, relacje z innymi ludźmi oraz aspekt umiejętności i nastawienia do hakingu. Użyli także przymiotnikowej skali własnego autorstwa opisującej cechy osobowości ankietowanych. Swoimi badaniami objęli hakerów z całego świata, głównie opierając się na kontaktach osobistych jednego z prowadzących projekt, który jest rozpoznawalnym w środowisku europejskim hakerem. W projekcie wzięło udział łącznie około 600 osób. Eksplorację rozpoczęto w 2004 roku, a jej zakończenie zaplanowano na rok 2012. Inne badania Chiesa, Ducci i Ciappi [12], jakkolwiek ciekawe, opierają się wyłącznie na ankiecie i nie uwzględniają aspektu kulturowego – niektóre dane demograficzne zaburzają wnioski końcowe, jak to ma miejsce w przypadku wykształcenia i hakingu czy też określenia siły ingerencji jednostek strzegących porządku prawnego w życie obywatela.

Jak wynika z analizy literatury przedmiotu, obecne badania nad subkulturą hakerską opierają się w większości przypadków na ankietach i kwestionariuszach nieuwzględniających zmiennych ubocznych, które często mogą całkowicie zmienić wartość wyników. Skupiając się na motywacji, ograniczają znaczenie czynnika osobowościowego, który decyduje o skuteczności i podejmowanych działaniach. Według wymienionych badaczy dominuje opinia, że hakerzy są osobami o różnych, często wykluczających się wzajemnie cechach osobowości, uzależnionymi od Internetu oraz o niskich kompetencjach społecznych. Takie podejście powoduje, że większość aktualnych badań oscyluje w granicach socjologii, mimo iż ich aspiracją jest tłumaczenie mechanizmów psychologicznych działań hakerskich. Kolejnym problemem jest traktowanie hakerów jako grupy homogenicznej, co również może w znaczącym stopniu spowodować zafałszowanie uzyskanych wyników. Wyjątkiem są tu badania Chantlera [3] i Rogersa [12], którzy proponują własne typologie hakerów, opierając się na kryterium umiejętności technicznych oraz motywacji.

3. Problematyka badań własnych

Jak wynika z prezentowanych wcześniej poglądów, szeroko rozumiana wiedza o technologiach IT (ang. information technology) oraz motywacja są czynnikami różnicującymi osoby popełniające przestępstwa komputerowe. Dla potrzeb tych badań przyjęto, że haker będzie

rozumiany jako osoba naruszająca integralność systemu komputerowego i posiadająca dostateczne umiejętności, aby wejść do systemu w sposób nieautoryzowany. Grupa sprawców nie jest jednak grupą homogeniczną. Za najtrafniejszą typologię należy uznać tę, która opiera się na aspekcie umiejętności technicznych. Wiąże się ona ze złożonością ataku i zdolnością do tworzenia własnych narzędzi. Za najważniejsze umiejętności świadczące o skuteczności hakera należy uznać: znajomość języków programowania, systemów operacyjnych oraz zagadnień związanych z bezpieczeństwem sieci. Założenie to stanowi punkt wyjścia do wyróżnienia grup sprawców. Celem badań jest odpowiedź na pytanie o heterogeniczność hakerów oraz wykazanie, czy i jakie cechy osobowości, kompetencje społeczne oraz uzależnienie od Internetu różnicują członków tej społeczności. Analiza literatury przedmiotu pozwala na postawienie hipotezy o heterogeniczności grupy i możliwości wyróżnienia przynajmniej dwóch podklas różniących się od siebie umiejętnościami hakerskimi. Przewiduje się także istnienie istotnych statystycznie różnic pomiędzy grupami w obrębie cech osobowości, kompetencji społecznych oraz uzależnienia od Internetu.

4. Osoby badane

Badaniami zostały objęte osoby, które popełniły przestępstwa komputerowe, czyli dokonały wielokrotnych nieautoryzowanych wejść do systemów komputerowych bez zgody ich właściciela. Osoby badane dobierano z pomocą specjalistów w dziedzinie technik IT i bezpieczeństwa sieci, pracujących najczęściej jako administratorzy sieci lub będących funkcjonariuszami służb mundurowych zajmującymi się ściganiem przestępstw komputerowych. Wskazywali oni znane im osoby posiadające w ich opinii wysokie umiejętności techniczne. W badaniach udział wzięły 422 osoby, z których do drugiej części dopuszczono 82. Tak duża różnica w liczbie osób badanych związana była z koniecznością wyeliminowania tych, którzy wypełniali testy w sposób tendencyjny lub nie spełniali kryterium głównego: dostatecznych umiejętności technicznych. Usunięto także wyniki osób, które nie wyraziły chęci udziału w drugiej części badań.

Osoby badane to w większości mężczyźni (95%). Udział kobiet był niewielki i wyniósł tylko 5%. Większość respondentów określiła swój wiek w przedziale 19–24 (41,5%) i 25–40 lat (45%). Ponad połowa z nich nie posiadała stałego partnera (58,5%), pozostali żyli w konkubinacie (19,5%) lub w związku małżeńskim (22%). Większość z nich (32,9%) mieszkała w średnim mieście oraz 40,2% w dużym. Pozostali badani zamieszkiwali małe miasta i wsie. Ponad połowa badanych miała wykształcenie niepełne wyższe i wyższe (71.9%).

5. Materiały i procedura badania

W celu weryfikacji postawionych hipotez zastosowano ankietę obejmującą dane demograficzne, skalę umiejętności technicznych obejmującą wiedzę na temat takich zagadnień, jak języki programowania, inżynieria programowania, bazy danych, systemy operacyjne, zagadnienia sieciowe, narzędzia graficzne oraz inne programy. Z narzędzi psychologicznych zastosowano Kwestionariusz Osobowości NEO-FFI autorstwa Costy i McRae [21], Kwestionariusz Kompetencji Społecznych KKS Matczak [9] oraz test uzależnienia od Internetu (PUI) Young [10, 19, 20].

Badanie było dwuetapowe. Podczas pierwszego etapu osoba badana wypełniała umieszczone na stronie internetowej wywiad, skalę umiejętności technicznych oraz test PUI. Jeśli jej poziom umiejętności technicznych był odpowiedni dla warunków badania, proszono ją o udział w drugiej części badań, w której wypełniała w formie papierowej kwestionariusze NEO-FFI oraz KKS. Podobną procedurę badawczą zastosował Rogers [11], który szukał ochotników za pośrednictwem sieci i za jej pośrednictwem określał poziom wiedzy badanych. Wywiad oraz pozostałe testy miały charakter anonimowy i dobrowolny, o czym informowano uczestników na samym początku badań. Równocześnie osoba badana miała prawo odmówić uczestnictwa w drugiej części procedury.

6. Wyniki

Zastosowana metoda analizy skupień metodą *k*-średnich pozwoliła na wyróżnienie dwóch grup różniących się od siebie pod względem umiejętności technicznych. W poszczególnych podgrupach znalazło się 49 osób o niższych umiejętnościach technicznych, w drugiej 33 badanych o większej wiedzy z zakresu języków programowania, systemów operacyjnych oraz wiedzy z zakresu bezpieczeństwa systemów. Uzyskane wyniki potwierdziły wcześniejsze badania, które wskazują na niższą liczebność osób o wysokich umiejętnościach w stosunku do posiadających małą wiedzę [3]. Odnosząc się do literatury przedmiotu, pierwszą grupę określono jako neofitów, a osoby należące do drugiej jako elitę. Największe różnice międzygrupowe można było zauważyć w znajomości języków programowania, systemów operacyjnych oraz zagadnień sieciowych. Osoby z grupy elity wykazywały większe umiejętności w tym zakresie. Elita dużo lepiej programowała, była bardziej biegła w zakresie obsługi systemów operacyjnych oraz tajników posługiwania się siecią, w tym także metod jej zabezpieczania. W pozostałych umiejętnościach różnice były mniejsze, jednak wiedza elity przewyższała neofitów w każdej z kategorii.

Drugim problemem była zależność pomiędzy umiejętnościami a osobowością, kompetencjami społecznymi

oraz uzależnieniem od Internetu. W tabeli I i II zaprezentowano uzyskane wyniki.

Jak wskazują porównania międzygrupowe, istnieją istotne statystycznie różnice w obrębie neurotyczności, otwartości na doświadczenia oraz sumienności. Osoby należące do elity są mniej neurotyczne, przewyższają natomiast neofitów poziomem otwartości na doświadczenia oraz sumiennością. Pomiędzy badanymi grupami nie wykazano istotnych statystycznie różnic w obrębie kompetencji społecznych oraz uzależnienia od Internetu.

7. Dyskusja wyników

Założono, że hakerzy nie stanowią populacji jednorodnej, a za kryterium różnicujące przyjęto umiejętności techniczne. Znalazło to całkowite potwierdzenie; wskazano dwie grupy – osób o mniejszych i wyższych umiejętnościach. W badaniach nie uwzględniono włamujących się do systemów telefonicznych oraz twórców wirusów, uznając ich, wobec aktualnego rozwoju technologii IT, za grupę niedostatecznie reprezentatywną w stosunku do całości populacji. Wyróżniona dzięki analizom statystycznym liczebność osób przypisanych do poszczególnych grup pozostawała w zgodzie z wcześniejszymi badaniami nad tą populacją, które mówią o małej liczbie osób posiadających wysokie umiejętności techniczne w stosunku do osób o przeciętnej wiedzy z zakresu technologii IT [por. 3. 4].

Za najbardziej tożsamą z uzyskanymi wynikami uznano typologię zaproponowaną przez Chantlera [3]. Na jej podstawie pierwszą grupę określono mianem neofitów, drugą jako elitę. Założono przy tym, że trzecia grupa wskazana przez Chantlera, lamerzy, to osoby, które nie zakwalifikowały się do badań. Zostały one odrzucone w pierwszym etapie ze względu na zbyt niskie umiejętności techniczne lub też chęć zawyżenia swojej wiedzy. Można ją także odnieść do typologii Chiesa [4], w której dzieli on hakerów na wykorzystujących znane luki w systemie, hobbystów oraz użytkowników sieci lokalnej. Odnosząc ją do uzyskanych wyników, badani należeli do dwóch pierwszych grup według typologii Chiesa, czyli osób o umiejętnościach do dokonywania ataków opartych na upowszechnianych błędach systemów (neofici) oraz tych, którzy potrafią tworzyć własne narzędzia, a ich ataki są bardziej zróżnicowane, przy tym haking stanowi ich wieloletnią pasję (elita).

Wyróżnione grupy różnią się od siebie pod względem wiedzy o językach programowania, systemach operacyjnych oraz zasadach funkcjonowania sieci. W tych trzech kategoriach wykazano największe dysproporcje. Zaproponowana przez Rogersa [11, 12] typologia potwierdza przyjęte tezy, jednak obejmuje szersze zagadnienie związane także z motywacją. Wyróżnienie grup wskazuje także na fakt, iż ewolucji ulega nie tylko sam Internet w jego aspekcie technicznym, lecz także jego użytkownicy, nawet tak specyficzni w swoim sposobie działania, jak hakerzy. W początkowym okresie historii hakingu traktowano ich jako jednolitą grupę, podczas gdy obecny rozwój technik informacyjnych pozwala na wyróżnienie wśród nich osób o wyższym i niższym poziomie zaawansowania, co skutkuje ich sposobem zachowania się w sieci. Oczywiście możliwy jest późniejszy „awans" osoby z grupy niższej do wyższej, jednak w opinii Chantlera [3] dochodzi do tego w niewielu przypadkach. Warunkiem przejścia z grupy neofitów do elity jest ciągłe poszukiwanie nowych wyzwań i poszerzanie wiedzy. Decydującą cechą osobowości jest tu otwartość na doświadczenia. Nowe umiejętności powodują poszukiwanie adekwatnych zadań, co powoduje ciągły wzrost zainteresowania zagadnieniami hakingu i wiedzy z tego zakresu. Warunkuje to dopuszczenie do grupy elity [18]. Na potrzebę podwyższenia swojego statusu w hierarchii wskazują także Chiesa, Ducci i Ciappi [4]. Wśród motywów hakowania badani wskazywali właśnie ten powód.

Grupy różnią się od siebie pod względem umiejętności technicznych. Stanowi to kryterium doboru, zatem rozbieżność w zakresie posługiwania się językami programowania, systemami operacyjnymi oraz zagadnieniami dotyczącymi globalnej sieci komputerowej jest zdecydowanie wyższa w przypadku elity. Posiada ona także wyższą wiedzę w zakresie baz danych oraz programów graficznych. Oznacza to, że wysokie umiejętności techniczne elity obejmują nie tylko zagadnienia ściśle związane z hakingiem, lecz także z szeroko rozumianym oprogramowaniem. Wskazuje to na fakt, iż wiedza ogólna z zakresu informatyki, jaką jest znajomość języków programowania oraz systemów operacyjnych, skutkuje także wyższą skutecznością i umiejętnościami w zakresie szeroko rozumianego IT.

Zależność ta tłumaczy także wcześniejsze rozważania dotyczące opanowania pewnych programów w oparciu o współpracę z innymi ludźmi. Należy tu wskazać na fakt, iż zależność ta pojawia się wyłącznie w grupie neofitów, co oznacza, iż kontakt z innymi hakerami, być może poszukiwanie swego rodzaju mentora, sięganie do ich wiedzy i doświadczenia, stanowi jeden z niezbędnych elementów rozwoju technicznego tych osób. Wymaga to jednak od nich wysokiej samooceny oraz wewnętrznego umiejscowienia kontroli, która zdaniem Chantlera [3], wynika z dużych umiejętności technicznych. Potwierdzają to także Chiesa, Ducci i Ciappi [4], którzy zauważyli u części swoich badanych chęć zostania swego rodzaju opiekunem osoby mniej doświadczonej. Dodają, że pierwsze osiągnięcia wynikają z własnych doświadczeń uzyskiwanych metodą prób i błędów, jednak zdobycie bardziej zaawansowanej wiedzy wymaga pomocy lepszych technicznie hakerów. Z tego względu neofici dążą do tego rodzaju kontaktów, starając się konsultować swoje poczynania z bardziej doświadczonymi hakerami.

Drugi problem badawczy zakładał różnice pomiędzy badanymi grupami w obrębie cech osobowości, kompetencji społecznych oraz uzależnienia od Internetu. Znalazł on częściowe wyjaśnienie, gdyż grupy różniły się w zakresie cech osobowości, jednak nie stwierdzono wyników istotnych statystycznie w poziomie kompetencji społecznych i uzależnienia od Internetu. Elitę cechuje niższy poziom neurotyczności, wyższa otwartość na doświadczenia oraz sumienność. W oparciu o literaturę przedmiotu pozwala to wnioskować o sposobie funkcjonowania tych osób w sieci. Osoby o wyższej neurotyczności będą przejawiały więcej zachowań dążących do zachowania anonimowości w sieci, które jednak – w powiązaniu z niskimi umiejętnościami technicznymi – nie zawsze będą efektywne. Mogą także tworzyć więcej sieciowych tożsamości, a nawet podszywać się pod innych użytkowników [2]. Równocześnie będą nadużywać CMC (ang. computer mediated communication) i cenić ją wyżej niż komunikację bez pośrednictwa Internetu [1]. Będą nadwrażliwe i impulsywne w działaniu, co może prowadzić do popełniania błędów ułatwiających ich ujęcie przez organy ścigania.

Skuteczność i wysokie umiejętności techniczne mogą być osiągnięte przez osoby z dużą ciekawością poznawczą, zrównoważone emocjonalnie, przy tym zorganizowane i wytrwałe. Kluczową cechą jest otwartość na doświadczenia, szczególnie zaś na jeden z jej elementów – tolerancję na nowość [5]. Skuteczność aktywności hakerskiej wymaga ciągłego poszerzania wiedzy i zdolności do szybkiej adaptacji nowych technologii i metod działania. Podobnie wnioski pojawiają się w badaniach Chantlera [3], który stwierdził wyższy poziom kreatywności u osób należących do elity. Sukcesy tej grupy wiąże on także z ich wewnętrznym poczuciem kontroli. Analogicznie uważają Voiskounsky, Babeva i Smyslova [17], którzy opisywali badaną przez siebie grupę jako osoby o dużej ciekawości intelektualnej, dużym sprycie i szybko uczące się. Podobnie uważają Chiesa, Ducci i Ciappi [4], których badani to osoby kreatywne, bystre, a przy tym buntownicy i marzyciele. Do podobnych wniosków prowadzi analiza samoopisu hakerów, którzy określali siebie jako dociekliwych i z jednej strony leniwych, z drugiej zaś zaangażowanych. Ten dualizm stanowi prawdopodobnie kryterium różnicujące grupy [4]. Niewątpliwie otwartość na doświadczenia jest cechą kluczową dla skuteczności hakera. Równocześnie sukcesy w hakingu wymagają kompetencji oraz perfekcji, a także rozwagi w działaniu [5]. Osoby o wyższych umiejętnościach technicznych uważnie planują swoje działania, są ostrożne, a przez to nie pozwalają sobie na błędy. Potrafią przy tym długo czekać na znalezienie luki w systemie, który w tym momencie próbują złamać. Za słuszny należy uznać wniosek Chantlera [3], który twierdzi, że kluczem do sukcesu w hakingu jest połączenie kreatywności i uporu w dążeniu do celu. Według Costa i McRae [5], osoby sumienne to przy tym osoby skrupulatnie przestrzegające zasad moralnych.

Można także postawić hipotezę, iż cechy przeciwne do posiadanych przez elitę, a zatem lęk przed relacjami interpersonalnymi, brak potrzeby poszerzania swoich umiejętności oraz nieobowiązkowość cechuje grupę lamerów korzystających z cudzego oprogramowania w celu wyrządzenia jak największych szkód w systemie komputerowym ofiary.

Nie stwierdzono rozbieżności w kompetencjach społecznych osób badanych, co oznacza, że nie są one czynnikiem różnicującym grupy. Należy jednak przyjąć założenie, iż w powiązaniu z wynikami innych badań istnieją różnice w sposobie używania Internetu przez członków poszczególnych grup. Wyższy poziom neurotyzmu miał związek z rzadszym sięganiem po serwisy informacyjne [1] oraz używaniem sieci do rozrywki [13]. Oznacza to także, że obie grupy mogą stosować socjotechniki jako metodę pozyskiwania kluczowych dla nich danych. Należy jednak podkreślić, że przeciętny poziom kompetencji społecznych pozwala wnioskować, iż dla tych osób nie będzie to główna metoda włamań.

Uzyskane wyniki pozwoliły na wyróżnienie dwóch grup – neofitów i elitę. Ich cechy osobowości pozostają w zgodzie z cechami podawanymi przez aktualną literaturą przedmiotu. Jak pokazują przeprowadzone badania, ich zróżnicowanie polega jednak nie tylko na umiejętnościach technicznych, lecz również cechach osobowości, co pozwala, jak sugeruje Donato, wnioskować o ich sposobie zachowania się w sieci, wybieranych celach, stosowanych metodach, a nawet o skuteczności ataku [6]. Wydaje się, że wiedza ta może stanowić przesłankę do stworzenia profilu psychologicznego nieznanego sprawcy przestępstwa komputerowego, który pozwoli zawęzić obszar jego poszukiwań, szczególnie w sytuacji ataków z wewnątrz sieci.