Problems of Forensic Sciences 2005, LXI, 30–41

ISSN 1230-7483

PSYCHOLOGICAL CHARACTERISTICS OF PERSONS COMMITTING COMPUTER CRIMES

Jakub LICKIEWICZ

Department of General Psychology, Maria Curie-Skłodowska University, Lublin

Abstract

Nowadays, the Internet is used both for work and entertainment. However, the increasing popularity of this medium means that it has also become a target for criminal activities. People who commit such offences are referred to as hackers. This term was understood in various ways until, in the course of time, it achieved its present negative meaning. Various definitions and typologies of the term are given nowadays, aimed at facilitating understanding of this phenomenon. However, research carried out up till now indicates that hackers are not an internally homogenous group, which makes it difficult to define the personality features of a typical hacker. Due to the growing number of computer attacks, a new branch of legal sciences, computer forensics, has been set up, which deals with the creation of psychological profiles of criminals. Analogies between hacker attacks and other aggressive crimes are sought more and more frequently. In order to create an adequate profile, we should collect as much information as possible about the time and place of the event, and also the victim of the attack. Only in this manner will we be able to determine precisely the personality traits and motivation of the criminal.

Key words

Motivation; Profiling; Computer forensics.

Received 10 October 2005; accepted 26 October 2005

1. Introduction

The growth and development of information technologies mean that the computer is increasingly frequently becoming a tool used for both work and entertainment. The ensuing genesis of an "Internet community" has led to a situation where a person can increasingly easily communicate, convey their opinions and acquire knowledge without the necessity of leaving home. However, the encroachment of computers into everyday life has been accompanied by another (unfortunate) aspect of their use: the application of knowledge about information technology to commit crimes, especially for financial gain. Persons committing such crimes are known colloquially as hackers.

2. Evolution of the concept and definitions

The concept of the "hacker" has gone through a long evolution, starting off in the 1950's, when it meant a "skilled electronics engineer" [33]. After some time, the meaning of the term altered somewhat, no longer being restricted to a person's skill alone, but also encompassing "hackers' ethics", which guided the hackers and at the same time created a specific subculture [4, 15]. This subculture was based around principles relating to freedom of information and unrestricted access to software. Invoking these principles, hackers began to fight against commercialisation of software and the concealing of information on protected servers. In this period, the word "hacker" began to take on a pejorative meaning [4]. As the use of computers became more widespread, hackers began to

break through the security features of games, and then broadened their activities to applications and services linked to the Internet. Currently, as a result of transformations in this subculture, the hacker is generally perceived by the public as someone who breaks into (a computer application) [33].

As can be seen from the above deliberations, it is difficult to give an unambiguous definition of the term "hacker". This is connected with changes in its meaning over time, and also depends on the point of view of the person describing the committed act. It is possible to identify four main approaches to this problem [17]. Prosecuting organs and institutions dealing with network safety perceive hackers as criminals, whose actions are a threat to the efficient functioning of the Internet. The media, on the other hand, perceive hackers as freaks, who have unlimited access to all the mysteries of the network and almost unlimited possibilities, which they often make use of to destroy and steal data or money from banks. Hackers (themselves) see themselves as computer enthusiasts, aiming to improve their understanding of information technology and the Internet. They often see themselves as guards, without whom the safety of the network would be threatened [31]. The last group is people whose opinions on hackers are difficult to define precisely. They are strongly influenced by the media, which try to present hackers' actions in the most spectacular way.

Hackers' actions raise a number of ethical issues, relating to unauthorised access to systems and viewing of files, despite non-destruction of data. They (hackers) explain that they are only checking security or want to indicate weak points of a system. Schneier vividly illustrates the issue by drawing an analogy with an apartment in which the returning owner finds a note informing him/her that during his/her absence someone noticed that the kitchen door was open, entered and looked around, but stole nothing. Moreover, the note's author suggests that the door locks should be changed. Schneider asks if the apartment's owner has a right to feel wronged and if his/her property has been encroached on, even though nothing was stolen [28].

3. Classification of the phenomenon

The basic classification, most often encountered in the literature, is differentiation into hackers, crackers, and phreakers [2, 10, 13, 18]. The first are persons who want to "find out about a selected part of a programme needed for work, to search through and work out details of operational systems and check their possibilities" [6, p. 19]. Fotinger and Ziegler [8] add that hackers have principles respected in their milieu: they want to use their knowledge with good intentions, which is why they inform the public about errors they find in systems and security features that they have hacked through.

Crackers, on the other hand, rarely write their own programmes, and their main aim is to damage other people's computer systems. Real hackers think of them as lazy, irresponsible, and not very intelligent persons [22]. In this division, the criterion of differentiation between the two groups is the aim of their actions, which, in the case of the former, is the desire to study systems closely, whereas in the case of the latter (crackers), is to destroy them. Phreakers are persons who break into telephone networks. However, currently, the meaning of the term "hacker" has become much broader and may encompass the activities of crackers and phreakers [7].

Rogers [1999] claimed that a "taxonomy" of hackers could be drawn up based on the level of advancement and technical skills. Starting from the least skilled:

- tool kit/newbie, script kids – persons who have just started hacking, basing their activities on simple programmes written by others and on instructions one can find in the network (tool kit);
- cyberpunks, who can write their own simple programmes, but possess rather limited knowledge; they often commit illegal acts such as damaging web sites, spamming (sending unwanted e-mails), and even stealing credit card numbers;
- internals are often ex-workers of a company, whose attacks are based on an excellent knowledge of the security systems used. What is important is that they have also worked in information technology companies, hence the ease with which they undertake hacking activities. According to Power [21], 70% of criminal activities on the Internet have been caused by persons from this group;
- coders are characterised by excellent skills; they write programmes often also used by other, less skilled hackers;
- the "old guard" is made up of highly qualified persons, who try to act according to hackers' ethics. They are mostly interested in the cognitive aspect of hacking; however, they have no respect for other people's property.
- professional criminals and cyber terrorists are persons who commit crimes in the network for material or ideological reasons. This group poses the biggest threat to the Internet community. Rogers [23] also adds the possibility of the existence of an-

other group, political activists, whose activities are rather rare.

Chantler [3] divided hackers into three groups, based on their education, experience and motivation:

– the "elite", composed of intelligent and well educated hackers, possessing great knowledge of programming. They often make use of less skilled hackers in their operations (all hackers studied by Chantler included themselves in this group, in spite of the fact that in his opinion they only constitute 30% of the examined population);
– "neophytes" brilliant, but not very well educated and often acting on the fringes of the law, using other people's programmes and needing more skilled hackers to guide them. Chantler observes that most hackers (60%) can be included in this group;
– young and inexperienced, often called "lamers" or "losers", they can be compared to "script kids". They often use tools and techniques with no understanding of the way in which they function. They mainly use their skills for financial gain, revenge or espionage. DoS (denial of service) attacks are typical of them, as they do not require more sophisticated skills [14].

Parker [20] formulated a classification of only those hackers who cause harm, and in this way he created profiles of cybercriminals:

– pranksters – persons who play various tricks on other network users; they can be thought of as sorts of Internet jokers, often harming other Internet users;
– hacksters browse through other people's computer systems out of curiosity, as a challenge or in the name of "social justice";
– malicious hackers are the equivalent of crackers; these terms are often used interchangeably in the literature, "malicious hackers" being applied when wishing to differentiate their activities from those of good hackers (see [12]);
– personal problem solvers constitute a group who become hackers when they fail to achieve some personal or professional aims in their real life;
– career criminals use their skills to gain material profits;
– extreme advocates are most often thought of as cyberterrorists, and they have very strong social, political or religious opinions;
– malcontents, addicts, irrational and incompetent persons, among whom there are many mentally ill persons.

Most of the classifications are based on the skills and aims of the particular persons who break into systems. It is worth noting that only a very limited group of hackers is able to create useful software; most of them use applications that have already been written without even trying to understand how they function.

4. Motivation

The motivation for hackers' activities is an aspect which provides very important information when trying to profile an unknown criminal. Frequently, there is a big difference between the declared motive for acting and the real reason for an attack. It is often characterised by a lot of aggression, although in interviews hackers claim their motives were curiosity or challenge, and only a few of them state that they broke in for material reasons or out of revenge. An example of a specific kind of vandalism may be breaking into web sites, a kind of Internet graffiti [24], which in no way can be justified by curiosity or intellectual challenge.

Vranesevich [36] tried to understand the motivation of hackers and listed the following kinds of motivation:

– social: thought to be one of the most common reasons for computer crimes. Hackers break into computers to gain the acceptance of a group, to feel superior, or to gain a feeling of control;
– technical: most hackers motivated by social reasons claim they are members of this group, whereas in fact technical motivation is rather rare. Technically motivated individuals hack – according to them – in order to contribute to the development of technology. They think that by breaking into computer systems of big companies or the military and pointing out their weaknesses, they will contribute to improvement of network safety;
– political: this is another type of motivation which people from the first group profess. They are individuals with strong political beliefs. They break into systems in order to disseminate their opinions. They frequently count on the interest of the press, which could help their "case". There is a fine line between political motivation and cyberterrorism, which is difficult to define. It is worth recalling, for instance, some mutual attacks of Palestinian and Israeli hackers on government systems of the enemy's country as a result of the Middle East conflict. Many authors also mention the transfer of political conflicts between Korea and Japan, Taiwan and China and China and USA to the Internet [5, 19];
– material: concerns people who hack for financial reasons; for example, they are industrial spies or

break into banks and big corporations. This group also includes people breaking through software security and computer pirates. Chantler [3] links the actions of this group with the self-esteem of its members, claiming that hackers with a low self-esteem are motivated "negatively" – they act out of revenge, for destructive reasons and have a low level of skills;
– governmental, which is linked with political motivation; this relates to espionage on behalf of a given country or "Internet wars".

As can be seen from the above classification, hackers are not a homogenous group in terms of motivation either. Many of them are not interested in political issues, but, as research by Woo et al. [34] shows, over 20% of web sites were "broken into" for political reasons, including nationalism, ethnic and religious conflicts.

Taylor [32] takes other factors into consideration in the motivation of hackers, stating that it is possible they coexist simultaneously. According to this author, these are:
– compulsive programming, connected with computer dependence and with the fact that a hacker must be up-to-date with continuous developments in information technology;
– hunger for knowledge connected with curiosity, which, according to Taylor, is the driving force for technological development. This author treats this as a positive need – thanks to this motivation, hackers test the limitations of current technologies;
– boredom, which is frequent among young hackers, for whom the level of computer science education at schools is unsatisfactory; as a result, they treat hacking into computers as an intellectual game. According to Taylor, involving these pupils in the education process often enables them to stop their criminal activities. Schwartau [27] notes that the current generation of hackers treats breaking in as a sport or a kind of game, which may confirm the motive of boredom among young hackers;
– the need for power connected with the fact that hacking into a server makes them feel better than the server's administrator; it also gives a feeling of having "defeated the system". The presence of this need in hackers helps us to understand why on web sites and in magazines on hacking, articles describing destructive activities, such as bomb construction can be found;
– the need for approval by the hacking community, thanks to which young hackers may socially interact with other people who understand and share their point of view; the existence of the hacking community also provides an opportunity for hackers to increase their self-esteem, because in this subculture skills matter [3]. Hackers also tend to boast about their capabilities, which shows their need for social approval;
– political actions; hacking may also be a kind of protest against social injustice, and, based on the principles of hackers' ethics concerning freedom of information, hackers may distribute information that is inaccessible to the public;
– opposition to bureaucracy and power; hackers often show their opposition to the dehumanisation of the bureaucratic system, in this way.

Hackers break into computer systems for various reasons, but it seems that an important factor is their age, social relations and their assessment of whether this activity satisfies needs that are indispensable for the proper functioning of an individual.

5. An attempt to formulate a psychological profile

Many researchers have tried to indicate characteristic traits, enabling the creation of a psychological profile of a hacker. Many of the results of conducted research contain inconsistent information on various personality traits. This is connected with the fact that the studied groups frequently differ in their race and age, as well as their motives for participating in the study. The profile presented below is based on a collection of data obtained during various researches, together with discussion of more important aspects of particular traits. According to these researches, a hacker:
– is a white man [24, 32]; however, according to research by Woo [34], Japanese and Koreans constitute a numerous group. At the same time, the number of women hackers is gradually increasing [22];
– is 12 28 years old [20, 34]; Chantler determined the age range of examined persons as 18 46, but their age is expected to continue falling [16]. Age is also connected with the ease with which young people acquire knowledge concerning use of computers [24];
– comes from a family of average wealth [32, 34]; Rogers [24] recognises this aspect as a risk factor, since appropriate funds are necessary in order to possess the necessary equipment. However, one can expect that with progress in technology, the importance of material status will gradually decrease;

– is often part of a one-parent family, with bad relations among its members [2, 25], which may have resulted in weak relations with other people and an attempt to replace them with a computer, and, furthermore, a lack of respect for authorities may also be a result,
– is an introvert with weak social skills, not functioning very well at school [3, 11, 17, 24]; however, this is not because of problems with learning, but because of difficulties with adapting to rules at school. Nevertheless, he/she has a need for social affiliation, which is realised by making the acquaintance of other hackers, whom s/he contacts *via* the Internet. The computer gives him a feeling of anonymity, thanks to which the relations are less threatening than with people in the real world;
– is skilled in information technology and is self-taught [17, 22]; the educational system does not provide him/her with enough knowledge, hence s/he searches for it by himself, mainly through exchange of information with other hackers;
– has symptoms of computer dependence, uses the network for a dozen or more hours per day [22], which may also mean that the computer is a method of escaping from reality for him/her.

It should be emphasised that the traits presented above relate to hackers regardless of the level of their skills, so they can also be applied to the "script kids" category. However, the authors also list the personal characteristics of persons with better technical skills, namely, using Rogers' classification [23], coders and people from higher categories. They are characterised by:

– high intelligence, creativity and cognitive curiosity [3, 22, 35]; however, as the example of script kids shows, these are not traits that are indispensable for an effective attack. For the majority of attackers use programmes created by others; these may be used without knowing how they work [23]. To be successful in this area, at least an average level of intelligence is needed [3];
– doggedness, concentration on details and analytical thinking [5, 12, 22, 25]. Hackers devote a lot of time and attention to becoming acquainted with the weak elements of the system which they want to break into. At the same time, they try to familiarise themselves with as many details as possible, since they believe they may turn out to be useful. They analyse obtained data very carefully and often work as long as needed to achieve their goal. In contrast to them, script kids quickly leave a system they cannot break into or use DoS attacks;
– specific moral system [3, 35], where there is a lack of differentiation between good and evil. Parker [20] noticed that a "Robin Hood syndrome" exists among hackers – breaking in is justified morally as a service to the community, and only wealthy companies are robbed. At the same time many hackers think that breaking into other people's computers without destroying or stealing of data is not morally reprehensible. They often blame network administrators for too weak protection of their servers [24];
– they create a specific hierarchy [3, 25] where knowledge and skills are very important; sometimes they co-operate in small groups composed of 6 7 persons, each person specialising in a different area. However, they are very cautious in making new contacts.

Shaw et al. [29] scrutinised a population of insiders, i.e. employees of companies who attack their own employers. Both current staff and ex-employees can be included in this category, and also partners from other companies. The researchers came to the conclusion that these hackers are persons with a tendency to feel negative emotions, disappointment, and as a result have disturbances of self-appraisal. Mostly, they are introverts with weak social skills and excessive self-esteem, and at the same time they have little empathy. At the same time they are addicted to the computer and have low feelings of loyalty.

6. Computer forensics

The frequency of crimes committed on the Internet has led to the establishment of a new field of science, referred to in the literature as cyber forensics or computer forensics, the aim of which is to help the administration of justice to catch computer criminals. This science does not concentrate only on the technical aspects of hacker's attacks, but also uses the achievements of many other forensic sciences, including investigative psychology, which in this area uses psychological knowledge in preliminary proceedings. Knowledge concerning the connections between personality and criminal behaviours is especially significant – this is one of the most important groups of problems in investigative psychology [9].

Similarities between classification of organised and disorganised murderers and classifications of computer criminals were noticed, based mainly on the place of the crime [12]. At the same time, on the basis of profiling principles, and, above all, studying the whole of the crime together with its context, a lot of in-

formation on the criminal's personality can be obtained. For example, Woo [34] notices that hackers tend to leave information on hacked websites concerning reasons for breaking in, information on the perpetrator, greetings to other hackers or emphasising their dislike of them and certain symbols. People use web sites to present themselves [34]. Hackers have a similar goal, changing other people's web sites according to their own wishes and leaving information on their own personality on such a site. To prepare an appropriate profile, it is essential to collect information on the time of hacking, sources of the attack and penetrated systems, methods of penetration and on browsed files [26, 30]. Collection of these data gives an opportunity to infer about the whereabouts, motivation and skills of the hacker. It is also emphasised that information obtained from the victim of the attack, interpreted using the science of victimology, is very important [26]. It is crucial to include the victim in the team of investigators, because this may significantly speed up the finding of the hacker, especially in cases in the "insider" category discussed above.

Computers, because of their prevalence, will increasingly be the targets of hacker's attacks. However, as one can conclude from the above, computer criminality is no longer solely the domain of security specialists; psychological knowledge is becoming increasingly important, with particular emphasis on profiling. The participation of a psychologist in the process of searching for an unknown hacker appears to be a necessity, because, against a background of continuously improving techniques of computer break-ins, the personality of the offender – focusing especially on motivation – is the only constant on which an investigator may rely.

References

1. Baught W. E. Jr., Denning D. E., Hiding crimes in cyberspace, [in:] Cybercrime, Loader B. D., Thomas D. [eds.], Routledge, Routledge 1999.
2. Białkowski M., Haking – przestępczość nowych czasów, *Przegląd Policyjny* 2002, 1, 138–148.
3. Chantler N., Risk: The profile of computer hacker, Curtin University of Technology, Perth 1996 [Ph.D. dissertation].
4. Chandler A., The changing definition and image of hackers in popular discourse, *International Journal of Sociology and Law* 1996, pp. 229–251.
5. Denning D. E., Activism, hactivism and cyberterrorism: The Interent as a tool for influencing foreign policy, [in:] Networks and netwars, Arquilla J., Ronfeldt D. [eds.], Rand, Santa Monica 2001.
6. Doroziński D., Hakerzy. Technoanarchiści cyberprzestrzeni, Helion, Gliwice 2001.
7. Duff L., Gardiner S., Computer crime in the global village: strategies for control and regulation in defence of the hacker, *International Journal of the Sociology of Law* 1996, 24, 221 228.
8. Fotinger C. S., Ziegler W., Understanding the hacker's mind a psychological insight into the hijacking of identities, Danube University Krems, Krems 2004.
9. Gierowski J. K., Określanie sylwetki psychofizycznej nieznanego sprawcy zabójstwa, [w:] Zabójcy i ich ofiary, Gierowski J. K., Jaśkiewicz-Obydzyńska T. [red.], Wydawnictwo Instytutu Ekspertyz Sądowych, Kraków 2002.
10. Godell J., Haker i samuraj, GWP, Gdańsk 1996.
11. Haffner K., Markoff J., Cyberpunks: outlaws and hackers on the computer frontier, Simon and Schluster, Toronto 1995.
12. Kleen L. J., Malicious hackers: a framework for analysis and case study, Air Force Institute of Technology, Ohio 2001.
13. Koerner I., Brendan I., Who are hackers, anyway?, *U.S. News & World Report* 1999, 126, 23.
14. Lesser I. O., Hoffman B., Arquilla J. [et al.], Countering the new terrorism, Rand, Santa Monica 1996.
15. Levy S., Hackers. Heroes of the computer revolution, Anchor Press/Doubleday, New York 1984.
16. Lickiewicz J., Obraz hakera w oczach uczniów szkół średnich, [w:] *Annales, Sectio J*, 2004 [w druku].
17. Lieberman B., Computer hackers. An intractable problem and what to do about it, Research and Policy Memorandum 301.1, Pittsburgh 2003.
18. Littman J., Ścigany. Rozmowy z Kevinem Mitnickiem, Helion, Gliwice 2004.
19. Paul L., When cyber hactivism meet cyberterrorism, http://www.sans.org/rr/ [stan na 12.02.2003].
20. Parker D., Fighting computer crime: A new framework for protecting information, John Wiley & Sons, New York 1998.
21. Power R., Current and future danger, Computer Security Institute, 1998.
22. Raymond, E., The new hacker's dictionary, http://home.nvg.org/~venaas/jargon/jargon_toc.html.
23. Rogers M., A new hacker's taxonomy, www.mts.net/mkr/hacker.doc.
24. Rogers M., A social learning theory and moral disengagement analysis of criminal computer behaviour: an exploratory study, Department of Psychology, University of Maniotoba 2001 [Ph.D. dissertation].
25. Schell B., Dodge J., The hacking of America: Who's doing it, why and how, Quorum, Greenwood 2002.
26. Schlarman S., Network intrusion management and profiling, [in:] Cyber forensic, Marcella A. J., Greenfield R. S. [eds.], CRC Press, Boca Raton 2002.
27. Schwartau W., Information warfare, Thunder Mouth Press, New York 2000.
28. Schneider B., The speed of security, *IEEE Security & Privacy*, 2003, 1, 96.

29. Shaw E., Ruby K., Post J., The insider threat to information systems: the psychology of the dangerous insider, *Security Awareness Bulletin* 1998, 2, 1–10.
30. Shinder D., Scene of cyber crime: Computer forensic handbook, Syngress Publishing, Rockland 2002.
31. Spafford E., Are hackers' break-ins ethical? [in:] Computers, ethics and society, Oxford, New York 1997.
32. Taylor P., Hackers. Crime in digital sublime, Routledge, New York 2000.
33. Williams S., W obronie wolności, Helion, Gliwice 2003.
34. Woo H. J., The hacker mentality, exploring the relationship between psychological variables and hacking activities, University of Georgia, Athens 2003 [Ph.D. dissertation].
35. 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.
36. Vranesevich J., How to be a hacker profiler, http://www.antionline.com/hacker-profiling/index.html.

Corresponding author
Jakub Lickiewicz
Uniwersytet im. Marii Curie-Skłodowskiej
Instytut Psychologii
Plac Litewski 5
20-080 Lublin
e-mail: jlickiewicz@op.pl

Problems of Forensic Sciences 2005, LXI, 30–41

CHARAKTERYSTYKA PSYCHOLOGICZNA OSÓB POPEŁNIAJĄCYCH PRZESTĘPSTWA KOMPUTEROWE

1. Wprowadzenie

Obecny rozwój technologii informatycznych sprawia, że komputer staje się coraz powszechniejszym narzędziem pracy i rozrywki. Idące za tym powstanie „społeczności internetowej" powoduje, iż jednostka z coraz większą łatwością może komunikować się, przekazywać swoje poglądy oraz nabywać wiedzę bez konieczności opuszczania miejsca zamieszkania. Jednak wraz z wkroczeniem komputerów w życie codziennie stopniowo pojawia się nowy aspekt ich funkcjonowania, którego najważniejszą cechą jest posługiwanie się wiedzą z zakresu informatyki w celu popełniania przestępstw, ze szczególnym uwzględnieniem uzyskiwania korzyści majątkowych. Osoby popełniające tego typu czyny karalne w języku potocznym określa się mianem hakerów.

2. Ewolucja pojęcia i definicje

Pojęcie „hakera" przeszło długą ewolucję, poczynając od lat 50. dwudziestego stulecia, gdy było ono równoważne ze „zdolnym elektronikiem" [33]. Wraz z upływem czasu, aby być hakerem, nie wystarczały same umiejętności, zaczęto coraz częściej mówić o etyce hakerskiej, która miała kierować postępowaniem i tym samym tworzyła z hakerów swoistą subkulturę [4, 15]. Zawierała się ona w zasadach, które dotyczyły głównie wolności informacji oraz swobodnego dostępu do oprogramowania. Powołując się na te zasady, hakerzy rozpoczęli walkę o nie, uważając, że nie można zezwolić na komercjalizację oprogramowania i ukrywanie informacji na zabezpieczonych serwerach. W tym okresie słowo „haker" zaczęło nabierać znaczenia pejoratywnego [4]. Wraz z upowszechnieniem komputerów hakerzy zaczęli łamać zabezpieczenia gier, aby potem rozszerzyć swoją działalność na aplikacje i usługi związane z Internetem. Obecnie, w skutek przemian, które zaszły w tej subkulturze, opinia publiczna utożsamia hakera z włamywaczem [33].

Jak wynika z powyższych rozważań, trudno jest jednoznacznie zdefiniować pojęcie hakera. Związane to jest ze zmianami jego znaczenia wraz z upływem czasu, ale także uzależnione jest od punktu widzenia osób, które podają definicję danego czynu. Można wyróżnić cztery główne podejścia do tego problemu [17]. Organy ścigania i organizacje zajmujące się bezpieczeństwem sieci widzą w hakerach przestępców, których działania stanowią zagrożenie dla sprawnego funkcjonowania Internetu. Z kolei media postrzegają ich jako dziwaków posiadających nieograniczony dostęp do wszelkich tajemnic sieci i niemal nieograniczone możliwości, które wykorzystują często do niszczenia i kradzieży danych lub pieniędzy z banków. Sami hakerzy postrzegają siebie jako entuzjastów komputerów, których celem jest coraz to lepsze poznawanie technologii komputerowej i Internetu. Często uważają się za strażników, bez których bezpieczeństwo sieci byłoby zagrożone [31]. Ostatnia grupa to osoby, których poglądy na hakerów są trudne do sprecyzowania. Największy wpływ mają na nich media starające się pokazać działania hakerów w sposób jak najbardziej widowiskowy.

Poczynania hakerów wywołują szereg etycznych problemów dotyczących nieautoryzowanego wchodzenia do systemu i przeglądania plików, pomimo nieniszczenia danych. Tłumaczą oni, że sprawdzają zabezpieczenia lub też chcą wskazać słabe punkty systemu. Schneier komentuje to obrazowym przykładem porównującym system do mieszkania, w którym po powrocie właściciel znajduje kartkę informującą, że w czasie jego nieobecności ktoś zauważył otwarte drzwi kuchenne, wszedł przez nie, rozejrzał się, ale nic nie zabrał. Następnie autor kartki sugeruje, aby naprawić zamki. Schneider stawia pytanie, czy właściciel mieszkania nie ma prawa czuć się pokrzywdzony i czy naruszono jego dobra, pomimo że nic mu nie skradziono? [28].

3. Klasyfikacje zjawiska

Podstawową klasyfikacją, najczęściej podawaną w literaturze przedmiotu, jest podział na hakerów, *crackerów* oraz *phreakerów* [2, 10, 13, 18]. Za tych pierwszych uważa się osoby, które chcą „poznać wybrany zakres programu niezbędnie potrzebny do pracy, zajmują się przeszukiwaniem i rozpracowywaniem szczegółów systemów operacyjnych oraz sprawdzaniem ich możliwości" [6, s. 19]. Fotinger i Ziegler [8] dodają, że hakerzy posiadają zasady, które są respektowane w ich środowisku, pragną używać swojej wiedzy w dobrych intencjach, stąd informują opinię publiczną o błędach, jakie znajdą w złamanych systemach i zabezpieczeniach.

W odróżnieniu od nich, *cracker* rzadko pisze własne programy, a jego celem jest uszkadzanie cudzych systemów komputerowych. Prawdziwi hakerzy uważają ich za osoby leniwe, nieodpowiedzialne i niezbyt błyskotliwe [22]. W tym podziale kryterium rozróżniające obie grupy stanowi cel ich działań, który u tych pierwszych stanowi chęć bliższego poznania systemów, pod-

czas gdy u *crackerów* niszczenia ich. *Phreakerzy* to osoby zajmujące się włamaniami do sieci telefonicznych. Jednak obecnie pojęcie „haker" jest dostatecznie ogólne, aby obejmować również działalność *crakerów* i *phreakerów* [7].

Rogers [1999] stwierdził, że opierając się na poziomie zaawansowania i umiejętności technicznych, można stworzyć taksonomię hakerów. Poczynając od najniższych umiejętności, są to:

– dzieciaki (*tool kit/newbie, script kids*), czyli osoby początkujące w „hakowaniu", bazują na wcześniej napisanym przez innych prostym oprogramowaniu i instrukcjach, które można znaleźć w sieci (*tool kit*);
– cyber-punki (*cyberpunks*) potrafiący napisać własne proste programy, lecz posiadający raczej ograniczoną wiedzę; często dokonują oni czynów zabronionych, takich jak: niszczenie stron internetowych, wysyłanie spamu (niechcianej poczty), a nawet kradzież numerów kart kredytowych;
– wewnętrzni (*internals*) to często byli pracownicy danej firmy, których ataki opierają się na doskonałej znajomości zastosowanych systemów zabezpieczeń. Istotne jest, że pracowali też w firmach komputerowych, stąd łatwość w podejmowaniu aktywności hakerskich. Power [21] stwierdza, że 70% kryminalnych działań w Internecie spowodowana została właśnie przez osoby z tej grupy;
– koderzy (*coders*) charakteryzują się wysokimi umiejętnościami, piszą programy, z których później korzystają inni, często mniej zaawansowani hakerzy;
– stara gwardia (*the old guard*) to osoby wysoko wykwalifikowane i starające się postępować zgodnie z zasadami etyki hakerskiej. Głównie interesuje ich poznawczy aspekt „hakowania", jednak cechuje ich brak szacunku dla cudzej własności.
– zawodowi kryminaliści (*professional criminals*) i cyberterroryści (*cyber terrorist*) to osoby, które dokonują przestępstw w sieci ze względów materialnych lub też ideologicznych. Grupa ta stanowi największe zagrożenie dla społeczności internetowej. Rogers [23] dodaje też możliwość istnienia kolejnej grupy, aktywistów politycznych, których działalność jest stosunkowo rzadka.

Chantler [3] dokonał podziału na trzy grupy, opierając się na wykształceniu osób należących do nich, ich doświadczeniu oraz motywacji:

– elita (*elite*), do której należą hakerzy inteligentni i dobrze wykształceni, posiadający dużą wiedzę na temat programowania. Często wykorzystują mniej doświadczonych hakerów w swoich działaniach (do tej grupy zaliczyli siebie wszyscy badani przez Chantera hakerzy, mimo iż jego zdaniem stanowią oni 30% badanej populacji);
– neofici (*neophytes*) błyskotliwi, ale o słabym wykształceniu i często działający na granicy prawa, używający cudzych programów i potrzebujący bardziej doświadczonych hakerów, którzy wskazaliby im sposób postępowania. Chantler zauważa, że większość hakerów (60%) zalicza się do tej grupy;
– młodociani i niedoświadczeni, często określani mianem lamerów (*lamers, losers*), których porównać można do kategorii *script kids*. Często stosują narzędzia i techniki, nie rozumiejąc sposobu ich funkcjonowania. Głównie używają swoich umiejętności do osiągnięcia zysków materialnych, zemsty lub szpiegostwa. Często stosują ataki typu DoS (*denial of service*), gdyż ich umiejętności nie pozwalają na bardziej specjalistyczne formy działania [14].

Parker [20] dokonał podziału hakerów wyłącznie czyniących szkody, tworząc w ten sposób profile cyberprzestępców:

– psotnicy (*pranksters*) to osoby, które stosują różne sztuczki w stosunku do innych użytkowników sieci, stanowią rodzaj internetowych żartownisiów, często szkodzącym innym;
– hakstersi (*hacksters*) przeglądają cudze systemy komputerowe z ciekawości, traktując to jak wyzwanie lub też w imieniu „sprawiedliwości społecznej";
– złośliwi hakerzy (*malicious hackers*) stanowią odpowiednik crackerów; co ważne, określenie to często pojawia się w literaturze zamiennie dla odróżnienia ich aktywności od dobrych hakerów (por. [12]);
– osoby rozwiązujące osobiste problemy (*personal problem solvers*) to grupa, która podejmuje aktywność hakerską, gdy nie udaje im się osiągnąć celów osobistych czy też zawodowych w życiu realnym;
– kryminaliści (*career criminals*) używają swoich umiejętności, aby uzyskać dobra materialne;
– ekstremalni obrońcy (*extreme advocates*) uważani są najczęściej za cyberterrorystów i posiadają mocno ukształtowane poglądy społeczne, polityczne lub religijne;
– malkontenci, uzależnieni, nieracjonalni, niekompetentni (*malcontents, addicts, irrational, incompetent*), wśród których często można znaleźć osoby chore psychicznie.

Większość podziałów opiera się na umiejętnościach oraz celach, jakie stawiają sobie poszczególne osoby, włamując się do systemów. Warto zauważyć, że tylko nieliczna grupa hakerów potrafi tworzyć przydatne w ich działalności oprogramowanie, podczas gdy większość korzysta z już działających aplikacji, nie starając się zrozumieć sposobu ich funkcjonowania.

4. Motywacja

Motywacja do działania jest tym aspektem działalności hakerów, który daje istotne informacje w późniejszej próbie profilowania nieznanego sprawcy. Zazwyczaj

istnieje duża rozbieżność pomiędzy deklarowanym motywem działania a rzeczywistym powodem ataku. Często cechuje go duża agresja, chociaż w wywiadach jako motywy swoich działań hakerzy podają ciekawość czy też wyzwanie i tylko pewna ich część twierdzi, że włamuje się ze względu na czynniki materialne lub zemstę. Przykładem swoistego wandalizmu może być włamywanie się na strony internetowe, rodzaj internetowego graffiti [24], którego w żaden sposób nie można uzasadnić ciekawością albo wyzwaniem intelektualnym.

Próbując zrozumieć motywację hakerów, Vranesevich [36] wyróżnił następujące motywacje:

– społeczna, uznana za jeden z najczęstszych powodów popełniania przestępstw komputerowych. Hakerzy włamują się do komputerów, aby zyskać akceptację grupy, dla poczucia wyższości lub też zyskania poczucia kontroli;
– techniczna; o przynależności do tej grupy stara się zapewnić większość osób „hakujących" z motywacji społecznej, podczas gdy w rzeczywistości jest to stosunkowo rzadko występujący motyw. Jednostki należące do tej grupy „hakują", aby w ich mniemaniu przyczynić się do rozwoju technologii. Uważają, że włamując się do systemów komputerowych dużych korporacji lub wojska i wskazując ich słabość, przyczynią się do poprawy bezpieczeństwa w sieci;
– polityczna; jest to kolejna motywacja, do której często przyznają się osoby z pierwszej grupy. Są to jednostki o silnych przekonaniach politycznych. Włamują się do systemów, aby ich poglądy stały się szeroko znane. Często liczą na zainteresowanie prasy, co może pomóc w ich „sprawie". Istnieje tu trudna do określenia granica pomiędzy motywacją polityczną a cyberterroryzmem. Warto przypomnieć choćby przykłady wzajemnych ataków hakerów palestyńskich i izraelskich na systemy rządowe krajów przeciwnych dokonywanych wskutek konfliktu na Bliskim Wschodzie. Wielu autorów wspomina również o przeniesieniu do Internetu konfliktów politycznych między Koreą i Japonią, Tajwanem i Chinami oraz Chinami i Stanami Zjednoczonymi [5, 19];
– materialna; dotyczy osób, które „hakują" dla uzyskania korzyści finansowych, np. uprawiają szpiegostwo przemysłowe czy dokonują włamań do banków oraz dużych korporacji. Do tej grupy zalicza się także osoby łamiące zabezpieczenia programów i piratów komputerowych. Chantler [3] wiąże działania tej grupy z samooceną jej członków, twierdząc, iż hakerów z niską samooceną cechuje motywacja „negatywna" zemsta, chęć czynienia szkód oraz niski poziom umiejętności;
– rządowa, która jest powiązana z motywacją polityczną; dotyczy działalności szpiegowskiej na rzecz danego kraju lub też „wojen internetowych".

Jak widać z powyższej klasyfikacji, także pod względem motywacji hakerzy nie są grupą homogeniczną. Wielu z nich nie interesuje się zagadnieniami politycznymi, jednak, jak wskazują badania Woo i współpracowników [34], ponad 20% stron internetowych zostało „złamanych" z pobudek politycznych, wliczając w to nacjonalizm, konflikty etniczne oraz religijne.

Taylor [32] uwzględnia inne czynniki w motywacji hakerów, stwierdzając, iż możliwe jest ich współwystępowanie w jednym czasie. W jego rozumieniu są to:

– przymus programowania związany z uzależnieniem od komputera oraz faktem, iż haker musi być obeznany z szybko zachodzącymi zmianami w technologii komputerowej;
– głód wiedzy powiązany z ciekawością, która, jak zauważa Taylor, jest kołem napędowym rozwoju technologii, traktując tę potrzebę jako pozytywną to dzięki niej hakerzy testują ograniczenia obecnych technologii;
– nuda będąca częstym zjawiskiem u młodych hakerów, dla których poziom edukacji informatycznej w szkołach nie jest satysfakcjonujący; w efekcie traktują oni włamania do komputerów jako zabawę intelektualną. Jak stwierdza Taylor, zaangażowanie tych uczniów w proces edukacji umożliwia często przerwanie przez te osoby działań przestępnych. Schwartau [27] zauważa, że współczesne pokolenie hakerów traktuje włamania jako sport lub swoistą grę, co może potwierdzać motyw nudy wśród młodych hakerów;
– potrzeba władzy związana z faktem, że włamanie do serwera pozwala im czuć się lepszym niż jego administrator, daje również poczucie „pokonania systemu". Obecność tej potrzeby u hakerów pomaga zrozumieć, dlaczego na stronach internetowych i w czasopismach dotyczących hakerstwa można znaleźć artykuły opisujące działania destrukcyjne, takich jak np. produkowanie ładunków wybuchowych;
– potrzeba uznania ze strony społeczności hakerskiej, dzięki której młodzi hakerzy mogą nawiązywać interakcje społeczne z innymi ludźmi rozumiejącymi i podzielającymi ich punkt widzenia; jest to także szansa na podwyższenie samooceny, gdyż w tej subkulturze znaczenie mają umiejętności [3]. Hakerzy mają też tendencję do chwalenia się swoimi osiągnięciami, co świadczy o potrzebie aprobaty społecznej;
– działania polityczne; hakerstwo może być bowiem także rodzajem protestu wobec niesprawiedliwości społecznej, a opierając się na zasadach etyki hakerskiej dotyczących wolności informacji, mogą oni upowszechniać informacje niedostępne opinii publicznej;
– sprzeciw w stosunku do biurokracji i władzy; hakerzy często okazują w ten sposób swój sprzeciw wobec dehumanizacji aparatu biurokratycznego.

Hakerzy włamują się do systemów komputerowych z różnych powodów, jednak istotnym czynnikiem wydaje się tu wiek, relacje społeczne oraz ocena, na ile ta działalność zaspokaja potrzeby niezbędne do prawidłowego funkcjonowania jednostki.

5. Próba sformułowania profilu psychologicznego hakera

Wielu badaczy starało się wskazać charakterystyczne cechy umożliwiające stworzenie psychologicznego profilu hakera. Wiele z wyników przeprowadzonych badań zawiera sprzeczne informacje na temat różnych cech osobowości. Związane jest to z faktem, iż badane grupy różnią się często rasą i wiekiem oraz motywacją do uczestnictwa w badaniu. Przedstawiony poniżej profil stanowi zbiór danych uzyskanych podczas różnych badań wraz z omówieniem ważniejszych aspektów poszczególnych cech. Według tych badań, haker:

- jest białym mężczyzną [24, 32], jednak jak wskazują badania Woo [34], wśród hakerów dużą grupę stanowią Japończycy i Koreańczycy. Równocześnie liczba kobiet wśród hakerów stopniowo wzrasta [22];
- ma 12 28 lat [20, 34], Chantler [3] określał przedział wieku osób badanych na 18 46 lat, jednak wiek będzie się wciąż obniżał [16]. Wiek związany jest również z łatwością, jaką mają młodzi ludzie w nabywaniu wiedzy dotyczącej posługiwania się komputerami [24];
- pochodzi ze średnio zamożnej rodziny [32, 34], Rogers [24] uważa ten aspekt za czynnik ryzyka, gdyż, aby posiadać odpowiedni sprzęt, konieczne są odpowiednie fundusze. Należy się jednak spodziewać, iż wraz z postępem technologii znaczenie statusu materialnego będzie stopniowo maleć;
- posiada rodzinę często z jednym rodzicem, a pomiędzy jej członkami istnieją złe relacje [3, 25], co mogło skutkować słabymi związkami z innymi i próbą ich zastąpienia przez komputer, przy tym także brakiem szacunku dla autorytetów;
- jest introwertykiem o słabych zdolnościach społecznych, słabo funkcjonującym w szkole [3, 11, 17, 24], jednak nie ze względu na problemy z nauką, ale trudności z dostosowaniem się do zasad panujących w miejscu ich edukacji. Posiada jednak potrzebę przynależności społecznej, którą realizuje przez znajomość z innymi hakerami, kontaktując się z nimi przy pomocy Internetu. Komputer daje mu poczucie anonimowości, dzięki czemu są to związki bezpieczniejsze niż z innymi ludźmi w świecie realnym;
- jest uzdolnionym informatycznie samoukiem [17, 22]; system edukacji nie dostarcza mu dostatecznej wiedzy, dlatego szuka jej sam, głównie poprzez wymianę informacji z innymi hakerami;
- ma objawy uzależnienia od komputera; korzysta z sieci przez kilkanaście godzin dziennie [22], co może także świadczyć o tym, iż komputer stanowi dla niego sposób na ucieczkę od rzeczywistych problemów.

Należy podkreślić, iż przedstawione wyżej cechy dotyczą hakerów bez względu na poziom ich uzdolnień, stąd można je odnieść także do kategorii *script kids*. Autorzy podają jednak cechy osobowości osób o większych umiejętnościach technicznych, czyli, odwołując się do klasyfikacji Rogersa [23], *koders* i osób z wyższych kategorii. Cechuje ich:

- wysoki poziom inteligencji, kreatywność oraz ciekawość poznawcza [3, 22, 35], jednak, jak wskazuje przykład *script kids*, nie jest to cecha niezbędna do przeprowadzenia skutecznego ataku. Większość atakujących korzysta bowiem z oprogramowania, które stworzyli inni; można go używać, nie znając jego działania [23]. Aby odnosić sukcesy w tej dziedzinie, konieczny jest przynajmniej przeciętny poziom inteligencji [3];
- upór w działaniu, orientacja na detale oraz analityczność myślenia [5, 12, 22, 25]. Hakerzy poświęcają dużo czasu i uwagi na poznanie słabych punktów systemu, który starają się złamać. Starają się przy tym poznać jak największą liczbę szczegółów, wierząc, że mogą się one okazać przydatne. Bardzo dokładnie analizują otrzymane dane i często pracują aż do osiągnięcia zamierzonego celu. W przeciwieństwie do nich, *script kids* szybko porzucają system, którego nie potrafią złamać lub też używają przeciwko niemu ataków typu DoS;
- specyficzny system moralny [3, 35], w którym brak jest rozróżnienia dobra od zła. Parker [20] zauważył wśród hakerów istnienie „syndromu Robin Hooda" polegającego na moralnym usprawiedliwianiu włamań jako służby dla społeczeństwa oraz dokonywaniu kradzieży wyłącznie od bogatych firm. Równocześnie wielu hakerów uważa, że włamywanie się do cudzych komputerów bez uszkadzania danych lub ich kradzieży nie stanowi niczego moralnie nagannego. Często obwiniają oni administratorów sieci za zbyt słabe zabezpieczenia swoich serwerów [24];
- tworzą specyficzną hierarchię [3, 25] w której znaczenie ma wiedza i umiejętności; czasem łączą się we współpracujące ze sobą grupy liczące 6 7 osób, w której każdy specjalizuje się w innej dziedzinie, są jednak bardzo ostrożni w nawiązywaniu nowych kontaktów.

Shaw i in. [29] zbadali populację „wewnętrzych" (*insiders*), czyli pracowników firm, którzy atakują własnych pracodawców. Do tej kategorii zaliczyć można zarówno obecnych, jak i byłych pracowników, a także partnerów z innych firm. Badacze ci stwierdzili, że są to osoby mające skłonność do odczuwania negatywnych

stanów emocjonalnych, poczucia rozczarowania, a w rezultacie zaburzeń oceniania. W większości są intorwertykami o słabych umiejętnościach społecznych i zbyt dużym poczuciu własnej wartości, przejawiają też słabe zdolności empatyczne. Równocześnie są to osoby uzależnione od komputera, o niskim poczuciu lojalności.

6. Informatyka sądowa

Częstotliwość przestępstw popełnianych w Internecie spowodowała powstanie nowej dziedziny wiedzy, informatyki sądowej, która ma ułatwić organom ścigania schwytanie przestępców komputerowych. Literatura anglojęzyczna określa ją mianem *cyber forensics* lub *computer forensics*. Nie jest to jednak nauka skupiająca się wyłącznie na technicznych aspektach ataku hakerskiego, lecz korzystająca z osiągnięć wielu dziedzin nauk sądowych, w tym psychologii śledczej, która w tym zakresie wykorzystuje wiedzę psychologiczną w toku postępowania przygotowawczego. Szczególnie istotna jest wiedza na temat związków pomiędzy osobowością a zachowaniami przestępczymi, co stanowi jedną z najważniejszych grup problemów wchodzących w zakres psychologii śledczej [9].

Zauważono podobieństwa pomiędzy podziałem na zabójców zorganizowanych i niezorganizowanych a klasyfikacjami przestępców komputerowych, opierając się głównie na miejscu popełnienia przestępstwa [12]. Równocześnie opieranie się na założeniach profilowania, a przede wszystkim na odczytywaniu całości zdarzenia wraz z jego kontekstem, pozwala na uzyskanie szeregu informacji dotyczących osobowości sprawcy tego czynu. Dla przykładu Woo [34] zauważa, że hakerzy mają tendencję do zostawiania na zmienionych stronach internetowych informacji dotyczących powodu ich złamania, wiadomości, kto to zrobił, pozdrowień dla innych hakerów lub też podkreślenia braku sympatii dla nich oraz pewnych symboli. Ludzie używają stron internetowych w celu autoprezentacji [34]. Podobny cel mają hakerzy, zmieniając posiadane przez innych strony według własnego uznania i zostawiając na takiej stronie informacje o swojej osobowości. Dla stworzenia prawidłowego profilu konieczne jest uzyskanie informacji na temat czasu włamania, źródła ataku oraz penetrowanych systemów, metody penetracji oraz penetrowanych plików [26, 30]. Zebranie tych danych daje możliwość wnioskowania o miejscu pobytu, motywacji oraz poziomie zaawansowania włamującego. Podkreśla się również znaczenie informacji, jakie można uzyskać od ofiary ataku, opierając się na osiągnięciach wiktymologii [26]. Istotne jest, aby włączyć pokrzywdzonego w skład ekipy poszukującej sprawcy, gdyż może to w znacznym stopniu przyśpieszyć jego znalezienie, jak to ma miejsce w przypadku omówionej powyżej kategorii „wewnętrznych" (*insiders*).

Komputery, ze względu na swoją powszechność, będą coraz częstszym obiektem ataków hakerskich. Jak jednak wskazują powyższe rozważania, przestępczość komputerowa przestaje być wyłącznie domeną specjalistów od zabezpieczeń, a coraz większą rolę odgrywa w niej także wiedza z zakresu psychologii, ze szczególnym uwzględnieniem profilowania. Uczestnictwo psychologa w procesie poszukiwania nieznanego sprawcy włamania do sieci wydaje się koniecznością, gdyż wśród wciąż wciąż udoskonalanych technik włamań komputerowych osobowość sprawcy, ze szczególnym uwzględnieniem jego motywacji, jest jedyną stałą, na której może oprzeć się śledczy.