Problems of Forensic Sciences 2011, vol. LXXXVII, 239–252

ISSN 1230-7483

CYBER CRIME PSYCHOLOGY – PROPOSAL OF AN OFFENDER PSYCHOLOGICAL PROFILE

Jakub LICKIEWICZ

Faculty of Health Sciences, Collegium Medicum, Jagiellonian University, Kraków, Poland
Faculty of Psychology and Family Sciences, Andrzej Frycz Modrzewski Krakow University, Kraków, Poland

Abstract

Cyber crime is an ever increasing threat to the security of computer systems. Break-in methods are becoming more and more sophisticated and complicated. This necessitates the use of complex security systems and makes it difficult – sometimes almost impossible – to catch offenders. This makes it necessary to search for new methods of hunting offenders, going beyond information technology methods. The present article concerns the issue of applying psychological profiling to the field of cyber crimes. A review of the literature is presented together with the author's theoretical model, which was created as a result of combining the Five Factor Theory (FFT) by Costa and McRae with psychological profiling methodology. The proposed construct assumes a relationship between psychological characteristics and the offender's modus operandi, which may serve in the creation of a psychological profile of a cyber crime perpetrator.

Key words

Psychological profiling; Cyber forensics; Hacker; Big Five Theory.

Received 19 May 2011; accepted 20 September 2011

1. Introduction

Information technology is currently one of the most dynamically developing fields in the world. The technological achievements of the internet seem to have outstripped the cognitive capabilities of the average user. Hand in hand with the dynamic development of the internet come threats linked with it. Widespread use of the internet is not unfortunately connected with knowledge of ways of protecting own data in the network. This results in increasingly frequent attacks on various computers, from simple one-user systems through bank systems to complex networks belonging to military structures. Attacks are carried out by persons perceived by the general public as hackers. However, this is a great generalisation, as the term "hacker" does not encompass cyber criminals [4]. As the literature points out, the former are different from ordinary cyber criminals in terms of numerous factors: motivation, ethical approach to own actions, and often abilities and technical skills [5, 18, 25].

2. Cyber criminality and methods of combating it

The necessity to secure and protect systems that are sensitive to attacks has resulted in the development of more and more complex security measures, as well as the creation of techniques which enable offenders to be caught. The reason such actions are so difficult is mainly the transnational nature of these types of crimes and the specificity of electronic evidence [16]. Attackers may be anywhere in the world, hiding their own actions through use of many computers, which

makes it significantly more difficult to locate them. As Stambaugh says, a specific characteristic of computer crimes is that it is "a scene of crime without a scene of crime" [35]. Moreover, usually a copy of the stored data, and not the original data itself is analysed. That is why the original evidence material should be stored in an unchanged state, and for the purpose of examination, a copy should be created on new and clean data carriers, using specialist equipment and software for this purpose [8].

The increasing widespreadness of the internet and at the same time ignorance of the risks linked with use of the internet have caused a rapid proliferation of crimes based on use of computers. The frequency of crimes committed in the network has led to the emergence of a new field, which aims to help law enforcement agencies to catch computer criminals. In the literature it is referred to as cyber forensics or computer forensics [23]. Sometimes, some authors use also the term digital forensics, understanding it as identification, collection, analysis and examination of electronic evidence, with preservation of integrity of data [15]. The Polish literature uses the term *inżynieria śledcza* (investigative engineering) or *informatyka śledcza* (investigative IT) or sometimes *informatyka kryminalistyczna* (forensic IT) to describe this field [24]. It is an area which combines criminalistics (forensics) and investigative methods in the recreation of a scene of crime. Its goal is prevention and detection and actions aimed at providing evidence that is necessary for penal proceedings to be conducted correctly [21]. Forensic engineering encompasses scientifically proven methods which make possible preservation, collection, approval, identification, analysis, interpretation, documentation and future presentation of digital evidence. Such evidence is obtained from electronic sources for the purpose of further reconstruction of events classified as crime or to prevent unauthorised actions aimed at changing or deleting evidence [2, 3]. Cyber forensics is a combination of numerous disciplines – from technical sciences, dealing with hardware and software, to legal, military and academic fields, encompassing both scientific research and education in this area. The role of the private sector is also important here, especially that of banks and corporations, which have a vital interest in achievements in this area [18].

In the face of so many difficulties in combating computer criminals, security specialists are increasingly interested in the only stable trait existing in such actions – the aggressors themselves and their personalities in the broadest sense of the word. A special role is played here by psychological profiling as a method used for drawing up a psychological description of an unknown offender. According to Gierowski, profiling falls within the scope of investigative psychology; it is a process which results in the creation of a short, dynamic profile, concisely describing the most important characteristics and manifestations of behaviour of an unknown perpetrator [14].

3. Psychological profiling in computer crimes

Psychological profiling is currently mainly used in murder cases [26]. In the case of computer crimes, psychological knowledge and experience can also certainly be applied. As Gierowski observes, such experience and knowledge allow us to interpret pieces of evidence collected at the scene in such a way as to enable us to determine the offender's personality type. This is based on the fact that according to basic rules of profiling there is a relation between an offender's personality and an act s/he committed. As a result, based on the method of operating (*modus operandi*) and traces left, one can infer about the psychophysical characteristics of an offender, including an offender's motivation and behaviour in the broadest sense [15]. Identical relations concern network attacks. As Rogers states, perpetrators of computer crimes count on the anonymity of the internet, but this anonymity does not concern their *modus operandi*, motivation and "signatures" they leave [29]. According to McQuade, each cyber criminal has his/her own techniques and software which s/he uses for break-ins [22]. Computer crimes are often of a serial nature, so it is possible to determine an offender's profile [1]. Erbschloe postulates the necessity of preparing profiles of perpetrators of internet terrorist attacks, considering them as an increasing threat to network security [12].

Profiling falls within the scope of applied psychology (investigative psychology is undoubtedly applied psychology). Representatives of this discipline also draw on numerous other disciplines, so one cannot, as some authors would have it, deny that it has the hallmarks of a science. Of great significance when preparing a profile is a data base, which, if properly prepared, allows information on perpetrators of similar crimes to be accumulated and enables scientists and investigators to search for analogies in future cases. Hence it is very important to constantly collect information which may be helpful in future law enforcement work.

Casey distinguishes two types of investigation in computer crime cases:

– a situation where a network incident occurred, but the offender's identity is not known, as in the case of network break-ins;

– a situation where both crime and offender are known, as for example in the case of catching a person possessing child pornography.

The author emphasises the usefulness of deductive profiling in both types of investigations in computer crimes [3]. One should, however, emphasise that it is difficult to talk about profiling of an offender in the second case mentioned by Casey. Referring to the definition of profiling as understood in investigative psychology (mentioned above), it consists in creation of a psychological profile of an unknown offender, and not a profile of a person who has already been arrested by law enforcement agencies.

Rogers claims that when creating a profile, one should analyse data in such a way as to be able to narrow down the search for persons to a certain group [28]. As a result, one can define the level of the offender's skills and his/her motivation. The profile should also include information on which area of the internet one should search for a given criminal (IRC channels, discussion groups). One should also thoroughly analyse a victim's actions on the internet and find the reason for the attack on the victim. This allows a more detailed profile of the offender to be drawn up and a future trap (honeypot) to be set for him/her [31]. Pleskonjić adds that when creating a profile it may be useful to make assumptions as to the offender's age and maturity, because it allows information to be gained on the offender's motivation, aims and culture in which s/he grew up [25]. The latter element may condition his/her behaviour and allow psycholinguistic methods to be used, which enable future identification of the offender in the case of further attacks.

As Casey says, profiling is helpful in explaining an offender's behaviour and the needs it fulfils. It may also enable determination of the place of operation of a given offender. Shaw suggests that a whole team – and not just a single profiler – is needed, composed of security specialists, internet technology specialists and lawyers. He also states that a profile is useful when one does not involve law enforcement agencies, when one tries to solve a case using one's own resources, which is especially significant when a given organisation wishes to avoid publicity [33]. Although Shaw does not mention a profiling team of psychologists in his proposal, as the present article shows, their role in profiling of an unknown computer crime perpetrator would be of key importance.

Shinder and Title indicate characteristics possessed by a cyber criminal:
– at least minimal technical skills;
– disrespect for legal norms and a feeling that one is outside their reach or beyond them;
– rich fantasy;
– a need to subordinate others and a tendency towards unnecessary risk;
– strong motivation, but of various types – from entertainment through a need to gain material goods to motives of a political character [34].

Similar characteristics of computer criminals are put forward by Chiesa, Ducci and Ciappi, indicating that:
– they have a higher than average intelligence quotient and high technical skills and abilities to solve problems;
– are "brilliant adolescents" [6, p. 22] bored by an inappropriate school system and poorly prepared teachers;
– they usually originate from pathological families;
– they rebel against all symbols and authorities [6].

The characteristics listed above constitute a basis for construction of a psychological profile of a hacker. Until now, several such attempts have been made using various methodology, often based on existing stereotypes.

4. Hacker profile model

Psychological profiling is a practical application of psychology and as such does not have its own, developed theoretical concept. To explain an individual's functioning, it is necessary to refer to a construct encompassing not just a selected range of human functioning, but a holistic concept (of human functioning). An example of such an understanding of an individual is the five-factor definition of personality in the FFT model (Five Factor Theory) by Costa and McCrae [3]. It encompasses a number of aspects connected with personality and factors that are dependent on it, which is why it seems to be reasonable to apply it to the concept of psychological profiling, as a global view of an offender. According to the authors of this concept, five personality traits are central elements, defined as basic tendencies: neuroticism, extroversion, openness, agreeableness and conscientiousness. Biological bases (traits), understood here as genetically determined individual characteristics, have an influence on the level of these factors. Characteristic adaptations, according to the authors, constitute another element, dependent on basic tendencies and external influences and thus culturally determined phenomena, personal aspirations and attitudes. An important element of this model is the assumption that despite the fact that this theory concentrates on personality characteristics, the following are also included among basic tendencies:

cognitive skills, artistic talents, sexual orientation and "all the psychological machinery lying at the basis of learning, perception and other psychological functions" [7, p. 223]. This means that this model can be included among holistic conceptions of human personality, encompassing the influence of both biological and social factors in its development. Whilst focusing on personality, at the same time, the significance of other psychological forces in the individual's functioning is not excluded. The researchers' concept is an open proposal, allowing one to grasp (individual) differences of an individual and is a basis for creating a theoretical model constituting an attempt to combine the FFT model and psychological profiling so as to adequately describe the phenomenon of computer criminality.

Costa and McCrae's model does not encompass aspects of criminal behaviour, especially the offender's *modus operandi*, whereas understanding of functioning of hackers also requires a holistic approach to this phenomenon. The literature provides numerous personality characteristics of offenders, yet they have no basis in any psychological construct. The construction of an adequate profile of a hacker needs to be based on theoretical assumptions which give a possibility of a holistic approach to an individual's activities, and hence the author's decision to choose the FFT model. Personality traits constitute only one of the elements (and not the most important one) conditioning the hacker's activities. That is why the author has built a theoretical model which could be a basis for further empirical examination. It has been named the "hacker profile model" and has been presented in graphical form in Figure 1.

The aim of the prepared model is to indicate relations between the offender's characteristics, environment and her/his success and the *modus operandi* during the attack. It assumes the existence of a dependence between the modus operandi of the perpetrator and central elements identified in him/her. This model was created on the basis of analysis of literature, taking into account hitherto demonstrated psychological relationships. It is based on assumptions which occur in the literature, concerning high intelligence, specific configuration of personality traits, low social skills, high technical skills and dependence on (addiction to) the internet. The above characteristics constitute the central element of the model. Although the existence of these types of indicators of hacking activity should be placed among stereotypes in thinking about persons committing computer crimes, they undoubtedly play a decisive role in the offender's success [34]. Results of previous research indicating the importance of these factors as important variables of hacker activities are a confirmation of the significance of central elements [3, 5, 29].

Two groups of factors have an influence on central elements:

1. Biological factors, namely a set of characteristics (properties) which take into account the physical traits of an individual, as well as injuries and genetic burdens, and past diseases. Previous results of research indicate their influence on the development of intelligence and personality [13]. There are also reports in the literature about dyslexia, dyscalculia, and even Asperger's syndrome occurring among hackers [39].
2. The external environment, encompassing widely understood environmental influences, and thus family influence, the upbringing and education process, relations with peers and siblings, as well as later functioning at school and at work. There are reports in the literature on bad relationships with parents and often divorces in hackers' families of origin [6]. Other researchers also write about difficulties at school, playing truant or abuse of psychoactive substances. The author of the present work assumes that the external environment influences the development of intelligence, personality, social skills, technical skills and degree of addiction to the internet [see: 10]. Studies by Costa and McRae in five cultures confirm this assumption [more: 7].

Five factors of equal importance make up the central elements:

1. Intelligence – understood here as ability to reason, analyse and think logically, which are an important element in the effectiveness of an attack. In the case of hackers' attacks, at least an average IQ is necessary, but it is also possible to break-in using such tools as special programmes downloaded from the network. The latter type of operation does not require a high intelligence quotient.
2. Personality – understood as a set of characteristics which are crucial for effectiveness of attacks. It should be emphasised that unlike Costa and McRae, the author understands it as an element that is equally important to other factors, but not the most important for a hacker's activities. Understanding these factors according to the earlier mentioned FFT theory, one may suppose that in the structure of this set of characteristics, of particular significance is the extroversion/introversion dimension, which determines the method of attack (use of technical methods or social influence techniques in the case of obtaining necessary information directly from a user). One may also hypothesise that a high level of neuroticism and openness to new experi-

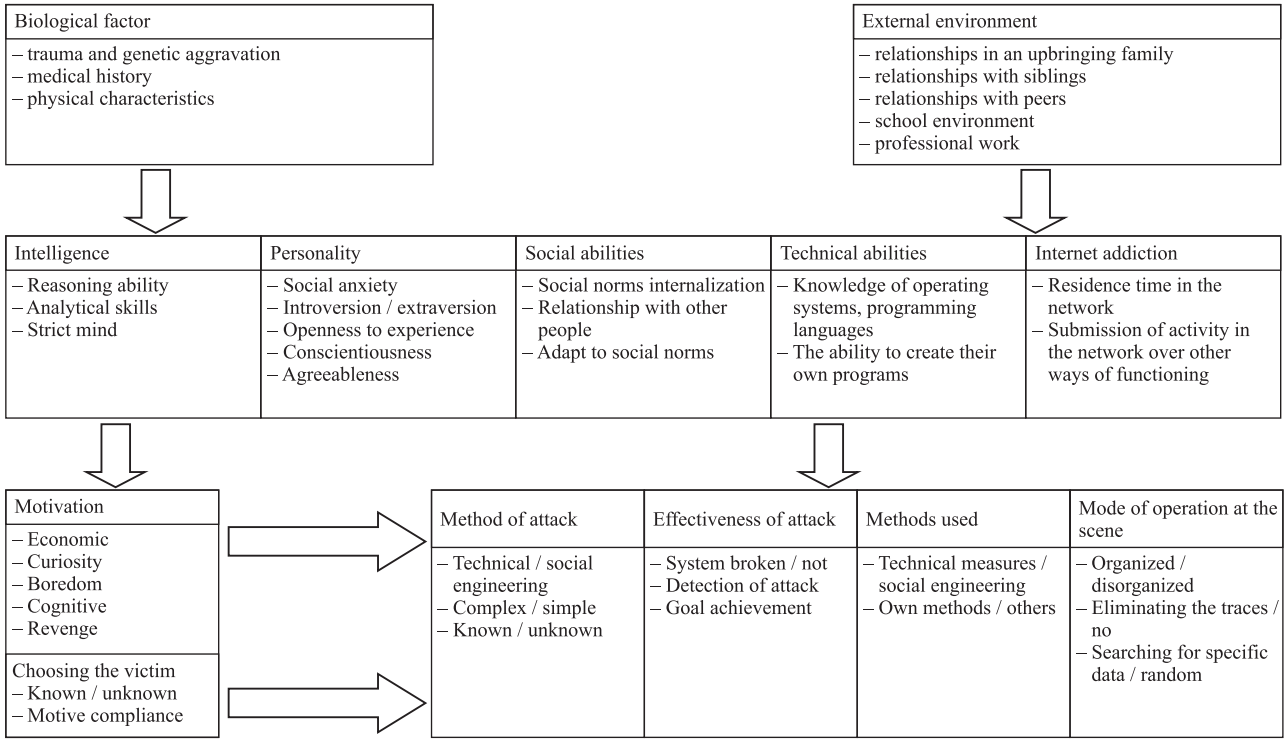

Fig. 1. Theoretical model profile of a hacker.

ences will be linked to strong motivation to act and aspiration to break the system. A high level of neuroticism may condition abuse of communication via the network, and also a strong need to maintain one's anonymity. One may suppose that openness to experiences determines being "up-to-date" – a need to learn new systems, as well as creativity and unconventionality in breaking security measures. In turn, one may assume that agreeableness and conscientiousness condition effectiveness at work and in fulfilling one's duties. According to the literature, both spheres are often neglected by hackers [33]. These characteristics are well illustrated by Shaw's studies. As transpires from his studies, insiders (employees breaking into servers at their own place of work) have a tendency to break the rules being in force at their place of work, ignoring superiors and coming into conflicts with them [9].

3. Social skills – they constitute a dimension which determines the individual's functioning in a group, internalisation of social norms and using them in private and professional life, and thus in broadly defined social adaptation. Social skills remain in relation to intelligence and technical skills. The literature emphasises the fact of low social skills among hackers, consisting in difficulties in relations with family and colleagues, sense of alienation and inability to form close interpersonal relations [9, 28, 33].
4. Technical skills – this element should be understood as general knowledge concerning programming languages, computer systems, network functioning (with special emphasis on network security), and also knowledge about other groups of applications used, among other things, for data base development. Information technology specialists draw attention to the necessity of knowing at least several programming languages (C, C++ and PERL are most frequently mentioned here) [see 9, 11]. According to Schell and Dodge, hackers should also know the principles of sending data through the network and at least two operating systems, one of which should be based on UNIX [30]. Knowledge in this area is crucial, because it allows them to make use of weaknesses of a system when breaking in [16].
5. Addiction to the internet – this element seems to be related to the effectiveness of an attack, but its presence is not necessary in all cases. Time devoted to computers may translate into skills in using them. The literature here talks about at least 50 hours per week spent after work on the internet [30, 36, 37].

There are a number of internal relations between central elements. The psychological literature indi-

cates correlations between intelligence and personality [32]. Intelligence also influences social and technical skills. There is a relation between personality and social skills that are related to abuse of the internet [7]. Social skills, apart from relations mentioned earlier, influence technical skills and addiction to the internet. Here there is also a relation between technical skills and abuse of the internet, but it does not manifest in all cases [7, 33, 37].

Central elements influence motivation to act, and this influences selection of a victim. On the basis of the literature discussed earlier, one may mention economic and political motives, curiosity, boredom or revenge [5]. However, one has to emphasise that the proposed typology is an intentional simplification of issues of motivation lying at the basis of computer crimes. One should assume that similarly to the case of the majority of other aggressive crimes, attacks on computer systems are characterised by multiple motives – in one criminal act one may distinguish several co-participating motives. The combination of growing technical skills and motivation may also be significant [38]. For this reason, motivation to act constitutes an independent element of the model, conditioning each activity of the individual. It determines selection of a victim, so on its basis, one may infer about the structure of central elements of a given offender. Among numerous concepts explaining motives of hackers, one may mention a proposal by Kilger et al. They propose a set of motives governing hackers' actions, which they term MEECES. This is an acronym created from the words: "money", "*ego*", "entertainment", "cause", "entrance into social groups" and "status". In such behaviour, an individual manifests their own needs, so appropriate establishment of motivation that is at the basis of actions is a key element when creating a profile [17]. This issue is dealt with more broadly by Reyes and Wiles, who distinguish three reasons why someone becomes a victim:

– something, that s/he physically possesses, e.g. fingerprints necessary to operate/activate a fingerprints scanner;
– something s/he knows, e.g. passwords, PIN codes etc.;
– something s/he has, e.g. entrance cards, credit cards [27].

Particular central elements will condition the method of attack, its effectiveness, methods used and behaviour at the scene of the crime and thus the offender's *modus operandi* [14]. One should emphasise here the direction of relations, from which it transpires that central elements influence other elements related to the offender's actions. Appropriate analysis of data from the crime scene allows us to infer about central elements. The possibility of applying this model in such a way indicates that it has a practical dimension. One should assume that relations occur between these elements, among which should be included:

– method of attack, which will be influenced by: intelligence, personality, social and technical skills. Intelligence and personality condition selection of methods. Social skills are important in the decision on use of technical means or social techniques during the attack. Technical skills influence methods used, including those developed by the hackers themselves;
– the effectiveness (success) of an attack, which is determined by intelligence, which is the most important element when working on breaking a system. Social skills may be important in the case of effectiveness of social techniques or when making use of other hackers' help. Technical skills will be important to master a system, which is related to knowledge of its weak sides;
– methods used, which are conditioned mainly by intelligence, personality and technical skills. Personality may be important in the case of break-in failure, because then an attack aimed at destruction of a system may be launched. A high level of social skills conditions use of social influence techniques;
– way of behaving at the scene of attack (understood here as a broken system), which is conditioned by the offender's intelligence and his/her ability to conceal traces at the scene of the crime. One may suppose that personality will determine methods of dealing with a broken system, whereas technical skills will determine how the hacker deals with the found data, and the effectiveness of execution of tasks set (by him/herself).

5. Summary

The model holistically encapsulates the actions of hackers and may be useful in the process of creation of a profile of an unknown perpetrator of computer crimes. According to a general rule of profiling suggested by Ressler: '"what" plus "why" equals "who"' allows reversal of the direction of inferring, and after collection of sufficient information at the scene of the incident allows one to define the characteristics making up the central elements of an offender [26]. As Białkowski says, attacks may be divided into technical ones and those using social influence [2]. The model takes into account both types of break-ins. What is

important here is that computer crimes are often of a serial nature, which allows collection of the required amount of data. One of the basic assumptions of psychological profiling is that the offender's method of operating (*modus operandi*) is connected with among other things his/her personality traits [14]. Collected data, concerning the effectiveness, used methods and behaviour at the scene of the incident thus allow us to infer about the characteristics constituting the central elements. A four-stage model of profiling by the FBI assumes collection of data, classification and reconstruction of a crime, and preparation of a profile. It seems that principles used for typing a sought person may also be useful in the case of computer crime [14]. That is why it is necessary to collect as much information as possible for the creation of a data base and for empirical confirmation of the accuracy of a hacker profile model. The developed model is a starting point for collecting this type of information, which will next be used in the creation of the hacker's profile.

The above mentioned model and the collated results of studies will be useful in drawing up a psychological profile of an unknown perpetrator of computer crime. It embraces a number of variables and factors which have not been analysed up till now in Polish literature. The theoretical model proposed in the present article is based on literature and constitutes a practical attempt to apply psychological knowledge, especially profiling of an unknown computer crime perpetrator. What is important is that this model is interdisciplinary in the sense that it combines knowledge on information technology and investigative psychology. One may also assume that it is culturally independent, because it attempts to explain offenders' behaviours irrespective of their origins and the cultural circle in which they function. Another important characteristic of this model is that it can be used without the necessity to collect additional data. During investigations carried out in cyber crime cases, one secures electronic evidence and all possible information concerning the place and time of attack and the methods used. This knowledge may be used in the creation of a psychological profile of an offender on the basis of his/her *modus operandi*. However, it should be emphasised that although a profile is not meant to indicate a specific aggressor, it helps to narrow down the search area, and also to define future approaches by law enforcement agencies and use of appropriate methods in order to quickly catch the offender. So it is advisable to consider a psychological profile in such types of crimes as a highly useful auxiliary tool.

References

1. Arkin O., Tracing hackers: A concept for tracing and profiling malicious computer attackers, *Computer Fraud & Security* 2002, 5, 8–11.
2. Białkowski M., Haking – przestępczość naszych czasów, *Przegląd Policyjny* 2002, 65, 138–148.
3. Casey E., Cyberpatterns: criminal behaviour on the internet, [in:] Criminal profiling. An introduction to behavioral evidence analysis, Turvey B. [ed.], Academic Press, San Diego 1999.
4. Chandler A., The changing definition and image of hackers in popular discourse, *International Journal of Sociology and Law* 1996, 229–251.
5. Chantler N., Risk: The profile of the computer hacker, University of Technology, Perth Curtin 1996.
6. 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.
7. Costa R., McCrae P., Osobowość dorosłego człowieka, Wydawnictwo WAM, Kraków 2005.
8. Cross M., Scene of the cybercrime, Syngress Publishing, Burlington 2008.
9. Doroziński D., Hakerzy. Technoanarchiści cyberprzestrzeni, Helion, Gliwice, 2001.
10. Drat-Ruszczak K., Oleś P., Osobowość, [w:] Psychologia akademicka, t. 1, Strelau J., Doliński D. [red.], GWP, Gdańsk 2009.
11. Erickson J., Hacking. The art of exploitation, Starch Press Inc., San Francisco 2008.
12. Erbschloe M., Information warfare. How to survive cyberattacks, McGraw Hill, New York 2001.
13. Gasiul H., Psychologia osobowości. Nurty, teorie, koncepcje, Difin, Warszawa 2006.
14. Gierowski J. K., Podstawowa problematyka psychologiczna w procesie karnym, [w:] Psychologia w postępowaniu karnym, Gierowski J. K., Jaśkiewicz-Obydzińska T., Najda M. [red.], Lexis Nexis, Warszawa 2010.
15. Grance T., Chevalier S., Kent K. [et al.], Guide to computer and network data analysis: applying forensic techniques to incident response, Computer Security Division, Gaithersburg 2005.
16. Graves K. [red.], Ethical hacking and countermeasures: Linux, Macintosh and Mobile Systems, Cengage Learning, Clifton Park 2010.
17. Kilger M., Arkin O., Stutzman J., Profiling. In the honeynet project know your enemy: learning about security threats, Addison Wesley, Boston 2004.
18. Ksherti N., Positive externality, increasing returns, and the rise in cybercrimes, *Communications of the ACM* 2009, 52, 141–144.
19. Lach A., Europejska współpraca w zwalczaniu cyberprzestępczości, [w:] Przestępczość teleinformatyczna. Materiały seminaryjne, Kosiński J. [red.], Wydawnictwo WSPol, Szczytno 2006.

20. Lickiewicz, J., Psychological characteristic of persons committing computer crimes, P*roblems of Forensic Sciences 2005*, 61, 30–37.
21. Mandia K., Prosise C., Incident response: Investigating computer crime, McGraw Hill, New York 2001.
22. McQuade S. C., Encyclopedia of cybercrime, Greenwood Press, London 2009.
23. McQuade S. C., Investigating and prosecuting cybercrime, [in:] Understanding and managing cybercrime, Pearson Education Inc., Boston 2006.
24. Moszczyński J., Informatyka kryminalistyczna, [w:] Kryminalistyka czyli rzecz o metodach śledczych, Goc M., E. Gruza E, Moszyński J. [red.], Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008.
25. Pleskonjić D., Milutinović V., Maček N. [et. al.], Psychological profile of network intruder, Conference IPSI, 23–26.03.2006, Amalfi, Italy.
26. Ressler R., Criminal personality profiling, *Problems of Forensic Sciences* 1997, 35, 32–41.
27. Reyes A., Wiles J., Best damn cybercrime and digital forensic book, Syngress Publishing, Burlington 2007.
28. Rogers M., A social learning theory and moral disengagement analysis of criminal computer behaviour: an exploratory study, University of Manitoba, Manitoba 2001.
29. Rogers M., A two dimensional circumplex approach to the development of a hacker taxonomy, *Digital Investigation* 2006, 3, 97–102.
30. Schell B., Dodge J., The hacking of America: Who's doing it, why and how, Quorum, Greenwood 2002.
31. Schell B., Martin C., Webster's new world hacker dictionary, Wiley Publishing Inc., Indianapolis 2006.
32. Schermer J. A., Vernon P. A., The correlation between general intelligence (g), a general factor of personality (GFP), and social desirability, *Personality & Individual Differences* 2010, 48, 2, 187–189.
33. Shaw E., The role of behavioral research and profiling in malicious cyber insider investigation, *Digital Investigation* 2006, 3, 20–31.
34. Shinder D. L., Tittel E., Cyberprzestępczość, Helion, Gliwice 2004.
35. Stambaugh H., Beaupre D., Icove D. [et. al.], Electronic crime needs assessment for state and local law enforcement, National Institute of Justice Washington 2001.
36. Weinstein A., Lejoyeux M., Internet addiction or excessive Internet use, *The American Journal of Drug and Alcohol Abuse* 2010, 36, 277–283.
37. Young K. S., Internet addiction: A new clinical phenomenon and its consequences, *American Behavioral Scientist* 2004, 48, 402–415.
38. Voiskounsky A. E., Smyslova O. V., Flow-based model of computer hackers motivation, *Cyberpsychology & Behaviour* 2006, 6, 2, 171–180.
39. Ziegler W., Fotinger C., Understanding the hackers mind – a psychological insight into the hijacking of identities, Danube University, Krems 2004.

Corresponding author
Dr Jakub Lickiewicz
Zakład Psychologii Zdrowia CM UJ
ul. Kopernika 25
PL 31-501 Kraków
e-mail: jlickiewicz@op.pl

Problems of Forensic Sciences 2011, vol. LXXXVII, 239–252

PSYCHOLOGIA PRZESTĘPCZOŚCI KOMPUTEROWEJ – PROPOZYCJA PROFILU PSYCHOLOGICZNEGO SPRAWCY

1. Wprowadzenie

Technologie informatyczne są obecnie jedną z najbardziej dynamicznie rozwijających się dziedzin na świecie. Osiągnięcia techniczne internetu wydają się wyprzedzać możliwości poznawcze przeciętnego użytkownika. W parze z dynamicznym rozwojem sieci idą także z nią związane zagrożenia. Powszechne korzystanie z internetu nie wiąże się niestety ze znajomością sposobów zabezpieczenia swoich danych w sieci. Powoduje to coraz częstsze ataki na różnego rodzaju komputery, od prostych systemów zwykłych użytkowników, przez systemy bankowe, po skomplikowane sieci należące do struktur wojskowych. Ataków dokonują osoby utożsamiane w opinii publicznej z hakerami. Jest to jednak duże uogólnienie, ponieważ nie można rozszerzać pojęcia hakera na sprawcę przestępstwa komputerowego [4, 20]. Jak wskazuje literatura przedmiotu, ci pierwsi różnią się od zwykłych internetowych przestępców wieloma czynnikami: motywacją, etycznym podejściem do swoich działań, a często zdolnościami i umiejętnościami technicznymi [5, 22, 29].

2. Przestępczość komputerowa i metody jej zwalczania

Konieczność zabezpieczania i chronienia wrażliwych na ataki systemów powoduje tworzenie coraz to bardziej złożonych zabezpieczeń, a także tworzenie technik umożliwiających ujęcie sprawców ataków. Trudność tych działań polega głównie na transgraniczności tego typu przestępstw oraz specyfice dowodu elektronicznego [19]. Sprawca może znajdować się w każdym zakątku globu, ukrywając swoje działania poprzez używanie wielu komputerów, co znacząco utrudnia jego zlokalizowanie. Jak stwierdza Stambaugh, specyfiką przestępstw komputerowych jest fakt, iż „jest to miejsce zbrodni bez miejsca zbrodni" [35]. Przy tym analizom podlega najczęściej nie oryginał, lecz kopia zapisów. Dlatego też oryginał dowodu powinien być zachowany w niezmienionym stanie, a na potrzeby badań należy stworzyć jego kopię na nowych i czystych nośnikach, używając przy tym specjalistycznego sprzętu i oprogramowania [8].

Rozszerzanie się zasięgu, a równocześnie nieznajomość zagrożeń związanych z korzystaniem z internetu, spowodowały szybkie pojawienie się przestępstw, które opierały się na wykorzystaniu komputerów. Częstotliwość przestępstw popełnianych w sieci wymusiła powstanie nowej dziedziny wiedzy, która ma pomóc organom ścigania w schwytaniu przestępców komputerowych. Literatura określa ją mianem *cyber forensics* lub *computer forensics* [23]. Czasem niektórzy autorzy używają także określenia digital forensics, rozumiejąc je jako identyfikację, zbieranie, analizę oraz badanie dowodów elektronicznych przy zachowaniu integralności danych [15]. Literatura polska stosuje tu określenie „inżynieria śledcza" lub „informatyka śledcza", czasem „informatyka kryminalistyczna" [24]. Jest to dziedzina, która łączy w sobie kryminalistykę i metody śledcze, odtwarzając miejsce przestępstwa. Jej celem jest prewencja, wykrywanie oraz działania zmierzające do dostarczenia dowodów niezbędnych do prawidłowego przebiegu procesu sądowego [21]. Inżynieria sądowa obejmuje naukowo udowodnione metody, które umożliwiają zachowanie, zebranie, zatwierdzenie, identyfikację, analizę, interpretację, udokumentowanie oraz późniejsze przedstawienie dowodów cyfrowych. Uzyskuje się je w celu umożliwienia dalszej rekonstrukcji zdarzeń zaklasyfikowanych jako przestępstwo, lub też, aby zapobiec nieautoryzowanym działaniom zmierzającym do zmiany lub usunięcia dowodów [2, 3]. *Cyber forensics* łączy w sobie wiele nauk – od technicznych, zajmujących się sprzętem oraz oprogramowaniem, przez prawne, militarne oraz akademickie, obejmujące zarówno badania naukowe, jak i edukację w tym zakresie. Ważna jest tu także rola sektora prywatnego, szczególnie banków i korporacji, jako żywotnie zainteresowanych osiągnięciami w tej dziedzinie [18].

Wobec tak wielu trudności w walce ze sprawcami przestępstw komputerowych, specjaliści od spraw zabezpieczeń coraz częściej interesują się jedyną stałą, jaka istnieje w tego typu działaniach – samym agresorem i jego szeroko rozumianą osobowością. Szczególną rolę spełnia tu profilowanie psychologiczne jako metoda służąca określaniu sylwetki psychologicznej nieznanego sprawcy przestępstwa. Według Gierowskiego, profilowanie wchodzi w zakres psychologii śledczej; jest procesem, który prowadzi do powstania krótkiej, dynamicznej charakterystyki, zwięźle opisującej najważniejsze cechy i przejawy zachowania nieznanego sprawcy przestępstwa [14].

3. Profilowanie psychologiczne w przestępstwach komputerowych

Profilowanie psychologiczne współcześnie wykorzystywane jest najczęściej w sprawach o zabójstwa [26]. W przypadku przestępstw komputerowych z pewnością

może być także wykorzystana wiedza i doświadczenie psychologiczne. Jak uważa Gierowski, pozwalają one na taką interpretację dowodów z miejsca zdarzenia, która daje możność określenia typu osobowości sprawcy. Wynika to z faktu, że zgodnie z podstawowymi założeniami profilowania, istnieje związek osobowości sprawcy z popełnionym przez niego czynem. Dzięki temu można na podstawie sposobu działania i pozostawionych śladów wnioskować o cechach psychofizycznych sprawcy, w tym o motywacji, a także szeroko rozumianym zachowaniu [15]. Identyczne zależności dotyczą ataków w sieci. Jak stwierdza Rogers, sprawcy przestępstw komputerowych liczą na anonimowość internetu, jednak nie dotyczy ona ich *modus operandi*, motywacji oraz „podpisów", jakie zostawiają [29]. Jak twierdzi McQuade, każdy przestępca komputerowy ma ulubione techniki i programy, których używa w celu dokonania włamań [22]. Przestępstwa komputerowe posiadają często charakter seryjny, a zatem możliwe jest określenie profilu sprawcy [1]. Erbschloe postuluje konieczność tworzenia profili sprawców ataków terrorystycznych za pośrednictwem internetu, traktując je jako coraz większe zagrożenie dla bezpieczeństwa sieci [12].

Profilowanie wchodzi w zakres psychologii stosowanej, jaką niewątpliwie jest psychologia śledcza. Przedstawiciele tej dziedziny wiedzy korzystają przy tym z pomocy wielu innych dyscyplin, nie można zatem, jak sugerują niektórzy autorzy, odbierać jej znamion naukowości. Duże znaczenie w tworzeniu profilu ma baza danych, która, gdy jest prawidłowo skonstruowana, pozwala na gromadzenie informacji na temat sprawców podobnych przestępstw i szukania analogii w przyszłych sprawach. Stąd niezbędne jest ciągłe zbieranie informacji mogących ułatwić późniejszą pracę organów ścigania.

Casey wyróżnia dwa rodzaje dochodzeń w sprawach komputerowych:
- sytuację, w której zdarzył się incydent sieciowy, jednak tożsamość sprawcy nie jest znana, jak w przypadku włamań do sieci;
- sytuację, gdy zarówno przestępstwo, jaki i sprawca są znani, jak to jest np. w przypadku ujęcia osoby posiadającej pornografię dziecięcą.

Autor podkreśla przydatność profilowania dedukcyjnego w obu rodzajach śledztw w przestępstwach komputerowych [3]. Należy jednak podkreślić, iż trudno mówić o typowaniu sprawcy w drugim z wymienionych przez Caseya przypadków. Odwołując się do przedstawionej wcześniej definicji profilowania w rozumieniu psychologii śledczej, polega ono na tworzeniu sylwetki psychologicznej nieznanego sprawcy przestępstwa, a nie profilu osoby już zatrzymanej przez organy ścigania.

Rogers twierdzi, że tworząc profil, należy analizować dane w taki sposób, aby zawęzić poszukiwania osób do konkretnej grupy [28]. Dzięki temu można określić poziom umiejętności sprawcy oraz jego motywację. Profil powinien również uwzględniać, w jakim obszarze internetu należy szukać danego przestępcy (kanały IRC, grupy dyskusyjne). Należy również dokładnie przeanalizować działania ofiary w sieci oraz znaleźć przyczynę ataku na nią. Pozwala to na stworzenie dokładniejszego profilu sprawcy oraz późniejsze zastawienie na niego pułapki (tzw. *honeypot*) [31]. Pleskonjić dodaje, że przydatne w tworzeniu profilu może być poczynione założenie dotyczące wieku i dojrzałości sprawcy, gdyż pozwala na uzyskanie informacji na temat jego motywacji i celów oraz kultury, w jakiej się wychował [25]. Ten ostatni element może warunkować jego zachowanie oraz pozwala na użycie metod psycholingwistycznych, co umożliwia późniejszą identyfikację sprawcy w przypadku kolejnych ataków.

Jak podaje Casey, profilowanie jest pomocne w wyjaśnieniu zachowania przestępcy oraz potrzeb, jakie zaspokaja. Może także umożliwić określenie miejsca działania danego sprawcy. Shaw sugeruje konieczność pracy nie pojedynczego profilującego, lecz całego zespołu składającego się ze specjalistów od bezpieczeństwa, technologii internetowych oraz prawników. Stwierdza przy tym, iż profil jest przydatny w przypadku nieangażowania w sprawę organów ścigania, gdy próbuje się rozwiązać sprawę przy pomocy własnych środków, co ma znaczenie szczególne znaczenie wtedy, gdy dana organizacja chce uniknąć rozgłosu [33]. Jakkolwiek Shaw nie wymienia w swojej propozycji zespołu profilującego złożonego z psychologów, jak jednak wskazują niniejsze rozważania, ich rola w typowaniu nieznanego sprawcy przestępstwa komputerowego byłaby kluczowa.

Shinder i Title wskazują na cechy, które posiada cyberprzestępca:
- przynajmniej minimalna sprawność techniczna;
- lekceważący stosunek do norm prawnych i poczucie, że jest się poza ich zasięgiem lub też ponad nimi;
- bogata fantazja;
- potrzeba podporządkowywania sobie innych oraz tendencja do podejmowania zbędnego ryzyka;
- silna motywacja, jednak różnego rodzaju, od rozrywki poprzez chęć zdobycia dóbr materialnych, po motywy o charakterze politycznym [34].

Podobne cechy przestępców komputerowych podają Chiesa, Ducci i Ciappi, wskazując na fakt, że:
- mają oni wyższy niż przeciętny iloraz inteligencji i duże umiejętności techniczne oraz zdolności rozwiązywania problemów;
- są „błyskotliwymi adolescentami" [6, s. 22] znudzonymi przez nieodpowiedni system szkolny i źle przygotowanych nauczycieli;
- najczęściej pochodzą z rodzin patologicznych;
- buntują się przeciwko wszelkim symbolom i autorytetom [6].

Wymienione wyżej cechy stanowią podstawę do konstrukcji profilu psychologicznego hakera. Dotychczas

dokonano kilku takich prób z wykorzystaniem różnej metodologii, często opierając się na istniejących stereotypach.

4. Model profilu hakera

Profilowanie psychologiczne jest umiejętnością praktycznego zastosowania psychologii i jako takie nie posiada własnej, rozbudowanej koncepcji teoretycznej. Do wyjaśnienia funkcjonowania jednostki konieczne jest jednak odwołanie się do konstruktu ujmującego nie wybrany zakres funkcjonowania człowieka, lecz jego holistyczną koncepcję. Przykładem takiego rozumienia jednostki może być pięcioczynnikowe ujęcie osobowości w modelu FFT (ang. Five Factor Theory) Costy i McCrae'a [3]. Obejmuje ono szereg aspektów związanych z osobowością i czynników wchodzących z nią w zależności, dlatego wydaje się słuszne odniesienie jej do koncepcji profilowania psychologicznego jako globalnego spojrzenia na sprawcę. Według autorów tej koncepcji, elementami centralnymi określanymi mianem podstawowych tendencji, jest pięć cech osobowości: neurotyczność, ekstrawertyczność, otwartość, ugodowość oraz sumienność. Na poziom tych wymiarów mają wpływ podstawy biologiczne, rozumiane tu jako uwarunkowane genetycznie cechy jednostki. Kolejny element stanowią, jak to określają autorzy, charakterystyczne przystosowania, zależne od podstawowych tendencji oraz wpływów zewnętrznych, a zatem zjawiska uwarunkowane kulturowo, dążenia osobiste oraz postawy. Ważnym elementem tego modelu jest założenie, iż mimo koncentracji tej teorii na cechach osobowości, w skład podstawowych tendencji wchodzą także zdolności poznawcze, talenty artystyczne, orientacja seksualna oraz „cała machina psychiczna leżąca u podstaw uczenia, percepcji oraz innych funkcji psychicznych" [7, s. 223]. Oznacza to, iż model ten można zaliczyć do całościowych koncepcji osobowości człowieka, obejmujący oddziaływanie czynników zarówno biologicznych, jak i społecznych w jej kształtowaniu się. Koncentrując się na osobowości, równocześnie nie wyklucza się znaczenia innych sił psychicznych w funkcjonowaniu jednostki. Koncepcja badaczy jest propozycją otwartą, pozwalającą na uchwycenie różnic indywidualnych jednostki i stanowi podstawę do stworzenia teoretycznego modelu stanowiącego próbę połączenia modelu FFT i profilowania psychologicznego tak, aby w sposób adekwatny opisywały one zjawisko przestępczości komputerowej.

Model Costy i McCrae'a nie obejmuje aspektów zachowania przestępczego, szczególnie *modus operandi* sprawcy, podczas gdy zrozumienie funkcjonowania hakerów wymaga także holistycznego ujęcia tego zjawiska. Literatura przedmiotu podaje wiele cech osobowości sprawców, nie mają one jednak podstaw w żadnym konstrukcie psychologicznym. Skonstruowanie adekwatnego profilu hakera wymaga oparcia się na założeniach teoretycznych, które dają możliwość całościowego ujęcia aktywności jednostki, stąd decyzja autora pracy o wyborze modelu FFT. Cechy osobowości stanowią jedynie jeden z elementów (przy tym nie najważniejszy) warunkujących działania hakerskie. Dlatego autor skonstruował model teoretyczny, który mógłby stanowić podstawę dalszych badań empirycznych. Nazwany on został „modelem profilu hakera" i przedstawiono go w formie graficznej na rycinie 1.

Celem opracowanego modelu jest wskazanie zależności pomiędzy cechami sprawcy, środowiskiem a jego skutecznością i sposobem działania w czasie ataku. Zakłada on istnienie zależności pomiędzy *modus operandi* sprawcy a wyróżnionymi w nim elementami centralnymi. Model ten powstał w oparciu o analizę literatury przedmiotu, uwzględniając przy tym wykazane dotychczas zależności psychologiczne. Opiera się na założeniach, jakie pojawiają się w piśmiennictwie, a dotyczących wysokiej inteligencji, specyficznej konfiguracji cech osobowości, niskich zdolności społecznych, wysokich umiejętności technicznych oraz uzależnienia od internetu. Powyższe cechy składają się na element centralny modelu. Jakkolwiek istnienie tego typu wyznaczników aktywności hakerskiej należy zaliczyć do stereotypów w myśleniu o osobach popełniających przestępstwa komputerowe, to bez wątpienia decydują one o skuteczności sprawcy [34]. Jednakże potwierdzeniem znaczenia elementów centralnych są wyniki dotychczasowych badań wskazujących na wagę tych czynników jako istotnych zmiennych działań hakerskich [3, 5, 29].

Na elementy centralne mają wpływ dwie grupy czynników:

1. czynniki biologiczne, czyli zespół właściwości uwzględniających cechy fizyczne jednostki, a także urazy i obciążenia genetyczne oraz przebyte choroby. Dotychczasowe wyniki badań mówią o ich wpływie na kształtowanie się inteligencji oraz osobowości [13]. Literatura przedmiotu podaje także doniesienia o dysleksji, dyskalkulii, a nawet zespole Aspergera występującym u hakerów [39].
2. Środowisko zewnętrzne obejmujące szeroko rozumiane wpływy środowiskowe, a zatem zarówno oddziaływanie rodziny, przebieg procesu wychowania, relacje z rówieśnikami i rodzeństwem, jak i późniejsze funkcjonowanie w szkole oraz w pracy zawodowej. Literatura przedmiotu donosi o złych relacjach z rodzicami oraz częstych rozwodach w rodzinach pochodzenia hakerów [6]. Inni badacze piszą też o trudnościach szkolnych, wagarowaniu czy nadużywaniu substancji psychoaktywnych. Autor tej pracy przyjmuje, iż środowisko zewnętrzne ma wpływ na rozwój inteligencji, osobowości, zdolności społecznych, umiejętności technicznych oraz poziom uzależnienia od internetu

[por. 10]. Badania Costy i McCrae w pięciu kulturach potwierdzają to założenie [więcej: 7].

W skład elementów centralnych wchodzi pięć równorzędnych czynników:

1. Inteligencja – pojmowana tu jako zdolność rozumowania, analizowania oraz logicznego myślenia, które są elementem ważnym w skuteczności ataku. W przypadku ataków hakerskich konieczny jest przynajmniej przeciętny iloraz inteligencji, jednak jest również możliwe włamanie dzięki takim narzędziom, jak specjalne programy ściągane z sieci. Działanie tego typu nie wymaga zatem wysokiego ilorazu inteligencji.
2. Osobowość – ujęta jako zespół cech, które są niezbędne do skuteczności ataków. Należy podkreślić, iż w odróżnieniu od Costy i McCrae'a, autor traktuje je jako element równoważny z innymi czynnikami, a nie najważniejszy dla działań hakerskich. Ujmując te czynniki w nurcie wspomnianej wcześniej koncepcji FFT, można przypuszczać, że w strukturze tego zespołu cech szczególne znaczenie ma wymiar ekstrawersji/introwersji, który determinuje sposób przeprowadzenia ataku (zastosowanie metod technicznych lub socjotechnik w przypadku uzyskania niezbędnych informacji bezpośrednio od użytkownika). Można także postawić hipotezę, iż wysoki poziom neurotyzmu oraz otwartości na doświadczenia będą miały związek z silną motywacją do działania i dążeniem do złamania systemu. Wysoki poziom neurotyzmu może warunkować nadużywanie komunikacji za pośrednictwem sieci, a także silną potrzebę zachowania anonimowości. Można przypuszczać, że otwartość na doświadczenia decyduje o „byciu na bieżąco" – chęci poznawania nowych systemów, a także kreatywności i niekonwencjonalności w łamaniu zabezpieczeń. Z kolei można założyć, że ugodowość i sumienność warunkują efektywność w pracy zawodowej i w wypełnianiu obowiązków. W świetle literatury przedmiotu te dwie ostatnie sfery są często zaniedbywane przez hakerów [33]. Cechy te dobrze ilustrują badania Shawa. Jak wynika z jego badań, insiderzy (pracownicy firmy dokonujący włamań do serwerów we własnym miejscu zatrudnienia) mają tendencję do łamania zasad obowiązujących w miejscu pracy, ignorowania przełożonych oraz wchodzenia z nimi w konflikty [9].
3. Zdolności społeczne – stanowią wymiar, który decyduje o funkcjonowaniu jednostki w grupie, internalizacji norm społecznych i stosowaniu ich w życiu prywatnym oraz zawodowym, a zatem szeroko rozumianym dostosowaniu społecznym. Pozostaje on w zależności z inteligencją oraz uzdolnieniami technicznymi. Literatura przedmiotu podkreśla fakt niskich zdolności społecznych wśród hakerów polegających na trudnościach w relacjach z rodziną i współpracownikami, poczuciem wyobcowania i nieumiejętnością nawiązywania bliskich relacji interpersonalnych [9, 28, 33].
4. Umiejętności techniczne – element ten należy rozumieć jako ogólną wiedzę z zakresu języków programowania, systemów komputerowych, funkcjonowania sieci (ze szczególnym uwzględnieniem sposobów jej zabezpieczania), a także o innych grupach aplikacji służących m.in. do tworzeniu baz danych. Specjaliści z zakresu technologii informacyjnych zwracają uwagę na konieczność znajomości przynajmniej kilku języków programowania (najczęściej wymienia się tu języki C, C++ oraz PERL) [por. 9, 11]. Jak uważają Schell i Dodge, hakerzy powinni także znać zasady przesyłu danych za pośrednictwem sieci oraz przynajmniej dwa systemy operacyjne, z czego jeden oparty na UNIXie [30]. Wiedza z tego zakresu jest kluczowa, gdyż pozwala na wykorzystanie słabości systemu we włamaniach [16].
5. Uzależnienie od internetu – ten element wydaje się mieć związek ze skutecznością ataku, choć jego występowanie nie jest konieczne we wszystkich przypadkach. Czas poświęcony komputerom może przekładać się na umiejętności posługiwania się nimi. Literatura mówi tu o przynajmniej 50 godzinach tygodniowo spędzonych w internecie poza pracą zawodową [30, 36, 37].

Pomiędzy elementami centralnymi występuje szereg zależności wewnętrznych. Literatura psychologiczna wskazuje na korelacje pomiędzy inteligencją i osobowością [32]. Inteligencja wpływa także na zdolności społeczne i techniczne. Istnieje związek osobowości z umiejętnościami społecznymi, które są powiązane z nadużywaniem internetu [7]. Zdolności społeczne, oprócz wymienionych wcześniej zależności, mają wpływ na umiejętności techniczne oraz uzależnienie od sieci. Występuje tu również związek pomiędzy umiejętnościami technicznymi i nadużywaniem internetu, chociaż nie pojawia się on we wszystkich przypadkach [7, 33, 37].

Elementy centralne wpływają na motywację do działania, ta natomiast na wybór ofiary. W oparciu o wcześniej omówioną literaturę przedmiotu, można wymienić motyw ekonomiczny, polityczny, ciekawość, nudę czy też zemstę [5]. Należy jednak zdecydowanie podkreślić, iż zaproponowana typologia stanowi celowe uproszczenie zagadnień motywacji leżącej u podstaw przestępstw komputerowych. Należy tu przyjąć, iż podobnie jak w przypadku większości innych przestępstw agresywnych, ataki na systemy komputerowe cechuje polimotywacyjność – w jednym akcie przestępczym można wyróżnić kilka współuczestniczących motywów. Znaczenie może mieć także związek rosnących umiejętności technicznych i motywacji [38]. Z tego względu motywacja do działania stanowi niezależny element modelu, warunkujący każdą aktywność jednostki. Determinuje ona wybór ofiary, a zatem na jej podstawie możemy wniosko-

wać o strukturze elementów centralnych danego sprawcy. Wśród wielu koncepcji tłumaczących motywy hakerów można wymienić propozycję Kilgera i współpracowników. Proponują oni zespół motywów rządzących działaniem hakerów, które określają jako MEECES. Jest to akronim powstały od słów „pieniądze" (ang. money), „*ego*", „rozrywka" (ang. entertainment), „powód" (ang. cause), „dostęp do grupy społecznej" (ang. entrance into social groups) i „status". Właśnie w działaniu jednostka ujawnia swoje potrzeby, zatem prawidłowe ustalenie motywacji leżącej u podłoża działania stanowi kluczowy element w tworzeniu profilu [17]. Zagadnienie to rozszerzają Reyes i Wiles, którzy wyróżniają trzy przyczyny, dla których obiekt staje się ofiarą:

- coś, co fizycznie posiada, np. odciski palców niezbędne do uruchomienia skanera linii papilarnych;
- coś, co wie, np. hasła, kody PIN itp.;
- coś, jest w jego posiadaniu, np. karty dostępu, karty kredytowe [27].

Poszczególne elementy centralne będą warunkować sposób ataku, jego skuteczność, stosowane metody oraz zachowanie na miejscu przestępstwa, a zatem *modus operandi* sprawcy [14]. Należy tu podkreślić kierunek zależności, z którego wynika wpływ elementów centralnych na pozostałe elementy związane z działaniem sprawcy. Odpowiednia analiza danych z miejsca zdarzenia pozwoli na wnioskowanie o elementach centralnych. W możliwości takiego zastosowania modelu leży jego wymiar praktyczny. Należy założyć, że pomiędzy tymi czynnikami występują zależności, do których należy zaliczyć:

- sposób ataku, na który będą miały wpływ: inteligencja, osobowość, zdolności społeczne oraz umiejętności techniczne. Inteligencja oraz osobowość warunkują dobór metod. Zdolności społeczne mają znaczenie w decyzji o użyciu podczas ataku środków technicznych lub socjotechnik. Umiejętności techniczne wpływają na używane metody, w tym także te własnego autorstwa;
- skuteczność ataku, o którym decyduje inteligencja będąca najważniejszym elementem w trakcie pracy nad złamaniem systemu. Zdolności społeczne mogą mieć znaczenie w przypadku skuteczności socjotechnik lub też korzystania z pomocy innych hakerów. Umiejętności techniczne będą istotne do opanowania systemu, z czym wiąże się znajomość jego słabych stron;
- stosowane metody, które uwarunkowane są głównie inteligencją, osobowością oraz umiejętnościami technicznymi. Osobowość może mieć znaczenie w przypadku niepowodzenia włamania, gdyż może być wtedy zastosowany atak służący zniszczeniu systemu. Wysoki poziom zdolności społecznych warunkuje użycie socjotechnik;
- sposób zachowania na miejscu ataku (rozumianym tu jako złamany system), który uwarunkowany jest inteligencją sprawcy oraz jego zdolnością do zacierania śladów na miejscu przestępstwa. Można przypuszczać, że osobowość będzie decydowała o sposobie działania ze złamanym systemem, natomiast umiejętności techniczne o postępowaniu ze znalezionymi danymi, a także o skuteczności wykonania stawianych sobie zadań.

5. Podsumowanie

Model ujmuje działania hakerów w sposób holistyczny i może być przydatny w procesie tworzenia profilu nieznanego sprawcy przestępstw komputerowych. Zgodnie ze wskazaną przez Resslera ogólną zasadą profilowania: „co" plus „dlaczego" równa się „kto", pozwala na odwrócenie kolejności wnioskowania, a po zebraniu dostatecznej liczby informacji na miejscu zdarzenia na określenie cech składających się na elementy centralne sprawcy [26]. Jak twierdzi Białkowski, ataki można podzielić na techniczne oraz socjotechniczne [2]. Model uwzględnia obie metody włamań. Znaczenie ma tu także fakt, iż przestępstwo komputerowe posiada najczęściej charakter seryjny, co pozwala na zebranie niezbędnej liczby danych. Jedno z podstawowych założeń profilowania psychologicznego mówi, iż sposób działania sprawcy wiąże się m.in. z cechami jego osobowości [14]. Zebrane dane o skuteczności, stosowanych metodach oraz działaniu na miejscu zdarzenia pozwalają zatem wnioskować o cechach należących do elementów centralnych. Czteroetapowy model profilowania FBI zakłada gromadzenie danych, klasyfikację i rekonstrukcję przestępstwa oraz tworzenie profilu. Wydaje się, że zasady stosowane do typowania osoby poszukiwanej mogą znaleźć zastosowanie także w przypadku przestępstwa komputerowego [14]. Dlatego też do opracowania bazy danych i empirycznego potwierdzenia prawdziwości modelu profilu hakera niezbędne jest zebranie jak największej liczby danych. Opracowany model stanowi punkt wyjścia do gromadzenia tego typu informacji, które następnie posłużą do stworzenia profilu hakera.

Wspomniany wyżej model oraz zebrane wyniki badań będą pomocne w określaniu sylwetki psychologicznej nieznanego sprawcy przestępstwa komputerowego. Obejmuje on szereg zmiennych i czynników, których dotychczas nie były analizowane w polskiej literaturze psychologicznej. Proponowany w niniejszym artykule model teoretyczny opiera się na piśmiennictwie i stanowi próbę praktycznego zastosowania wiedzy z zakresu psychologii, szczególnie profilowania w określaniu sylwetki psychologicznej nieznanego sprawcy przestępstwa komputerowego. Jego ważną cechą jest interdyscyplinarność polegająca na powiązaniu wiedzy z zakresu technologii informatycznych i psychologii śledczej. Można również założyć jego niezależność kulturową, gdyż stara się on tłumaczyć zachowania sprawców bez względu na miej-

sce ich pochodzenia i krąg kulturowy, w którym funkcjonują. Kolejną ważną cechą modelu jest możliwość jego zastosowania bez konieczności gromadzenia dodatkowych danych. W toku śledztwa prowadzonego w sprawach dotyczących przestępstw komputerowych zabezpiecza się dowody elektroniczne oraz wszystkie możliwe informacje dotyczące miejsca ataku, jego czasu i zastosowanych metod. Wiedza ta może także posłużyć stworzeniu sylwetki psychologicznej sprawcy na podstawie jego modus *operandi*. Należy jednak podkreślić, że jakkolwiek profil nie służy określeniu konkretnego agresora, to pomaga jednak zawęzić obszar poszukiwań, a także określić dalszy sposób postępowania organów ścigania i zastosowanie odpowiednich metod służących szybszemu ujęciu sprawcy. Wskazane jest więc traktowanie profilu psychologicznego w tego typu przestępstwach jako wysoce przydatnego narzędzia pomocniczego.