Do hackers need ethics?

Czy hakerzy potrzebują etyki?

***Przemysław Chmielecki**, Wyższe Baptystyczne Seminarium Teologiczne w Warszawie*

Typ artykułu: oryginalny artykuł naukowy.

Źródło finansowania badań i artykułu: środki własne Autora.

Cytowanie: Chmielecki P., (2018) *Do hackers need ethics?* „Rynek-Społeczeństwo-Kultura" nr specjalny (31)/2018, s. 80-82, https://kwartalnikrsk.pl/Artykuły/RSK-Specjalny-2018/RSK-Specjalny-2018-Chmielecki-Do-hackers-need-ethics.pdf

ABSTRACT

The goal of this article is to present the issue of hackers' ethical code and at least a few examples of its usage in practice. The author, as an IT professional and philosopher, wants to answer the question stated in the title: do hackers need ethics? At first comes the definition of hacker and examination of six points of Steven Levy's Hacker Ethics: (1) postulate of unlimited access to computers (2) and free admittance to information, (3) promotion of decentralization, (4) hackers should be judged by their hacking, (5) hacking as computing art, and (6) computers can change the life for better. The question is still valid - which ethics should hackers follow? They are on the boundaries of law, but their work is still needed, and hackers are not expelled from society. Hackers' tools are publicly available (for instance VPN, TOR, Kali-Linux), but the moral evaluation depends on chosen ethics. Even governments and big corporations ask for hackers' help in penetration tests and looking for security backdoors in applications. The aim of the author is to describe the ethical principles important for hackers and the assumptions behind them, as well as to make a moral evaluation of hacking actions.

Keywords: hacker, ethics, moral code.

STRESZCZENIE

Celem tego artykułu jest przedstawienie problemu kodeksu etycznego hakerów i przynajmniej kilku przykładów jego użycia w praktyce. Autor, jako specjalista IT oraz filozof, chciał odpowiedzieć na pytanie zawarte w tytule: czy hakerzy potrzebują etyki? Artykuł rozpoczyna próba zdefiniowania hakera i badanie sześciu punktów etyki hakerskiej wg. Stevena Levy'ego: (1) postulat nieograniczonego dostępu do komputerów (2) i swobodny dostęp do informacji, (3) promowanie decentralizacji, (4) hakerzy sądzeni za ich hakowanie, (5) hakowanie jako sztuka komputerowa, (6) komputery mogą zmienić życie na lepsze. Pytanie pozostaje aktualne – jaką etykę powinni stosować hakerzy? Lokują się na granicy prawa, ale ich praca jest nadal potrzebna i hakerzy nie są wydalani ze społeczeństwa. Narzędzia hakerskie są publicznie dostępne (np. VPN, TOR, Kali-Linux), ale ocena moralna działania zależy od wybranej etyki. Nawet rządy i wielkie korporacje proszą hakerów o pomoc w przeprowadzaniu testów penetracyjnych i szukaniu backdoorów bezpieczeństwa w aplikacjach. Celem, który stawia sobie autor, jest opisanie ważnych dla hakerów zasad etycznych oraz założeń, jakie za nimi stoją, a także dokonanie swoistej oceny moralnej czynów.

Słowa kluczowe: haker, etyka, kodeks moralny.

The history of utopias is no less fascinating
than the history of metallurgy or of chemical engineering
Leszek Kołakowski (1978: VI)

Hacker ethics have been discussed in many papers on a European and global scale. When you type "hackers" into WorldCat network library, the search will reveal almost twenty thousand books and nearly ninety thousand scientific articles in various journals. Among others, we can list Aase Berg and Johannes Göransson's *Hackers* (2017), Margaret Haerens and Lynn M. Zott's *Hacking and Hackers* (2014), Charlie Carter's *History Hackers* (2013), Jorge Alberto Lizama Mendoza's *Hackers* (2012), and Drew Conway and John Myles White's *Machine Learning for Hackers* (2012). Nevertheless, the most famous book related to the hackers' society is, now a classic, Steven Levy's *Hackers: Heroes of the Computer Revolution* (1984). It is the most important source of knowledge about hacker's ethics in this article, but not the only one. The ambition of the author is to show the hackers' concept of ethics, the main rules they follow, the rights which they defend and the morality of hacking individuum.

Who is a hacker?
Changing the image of cyber-anonymous

Currently, it is difficult to define the term "hacker" and "hacking". Based only on Internet research we can note that a hacker is "a person who illegally gains access to and sometimes tampers with information in a computer system" (merriam-webster.com 2018) or "a person who uses computers to gain unauthorized access to data" (oxforddictionaries.com 2018). Those hacker definitions have something in common and they are focused on unapproved access to someone's data. The Business Dictionary describes a hacker as "skilled computer programmer who breaks (hacks) a password code, or otherwise gains remote access to a protected computer system, mainly for the thrill of it. Unlike a 'cracker,' a hacker may or may not also perform a criminal action such as alteration or stealing of data, or transfer of funds" (businessdictionary.com 2018). Most commonly (and informally), a hacker is known as "an expert at programming and solving problems with a computer" (merriam-webster.com 2018). According to this statement, today everyone could be a hacker. Hacking is not a professional occupation but rather an opportunity to cross the security boundaries. Computer users who want to be a hacker can act in several ways – both ethical and non-ethical. The Urban Dictionary provides three classifications of hackers: (1) White-hat (hacking for the enjoyment of exploration), (2) Black-hat (hacking to find exploits and system weaknesses; cracker) and (3) and Grey-hat (someone who is a little of both) (urbandictionary.com 2018). Here we find the important distinction depending on one's internal moral code, which leads to the motivation and desired result of hacking.Based on presented definitions and for the purpose for this article, the term "hacker" should be understood as the person who gains access to other people's data (sometimes with the consent or at the request of this person) in a non-standard way (by breaking or bypassing the security mechanisms).

Hackers' Moral Code – is there such a thing?

In a natural way, it seems wrong to combine the words "hacker" and "morality" in one sentence. On the one hand, hackers associate with immorality, law breaking, the dark sphere of the Internet, etc. On the other hand, the difference between "ethics" and "morality" seems too blurry and not well distinguished. While the first one is generally linked with proper behavior according to law and social order, the second refers to a scientific subdiscipline related to general rules of moral behavior. The common understanding of ethics is wrong in the sense that it mismatches "ethics" with "morality". If morality is the set of human behaviors, how people act, what they do in general, then ethics is the set of moral acts evaluated in the axiological sense in accordance with the adopted criteria. Sometimes ethics could be enclosed in ordered code (Kołakowski 2009). Behavioral assessment as "moral" or "immoral" contains an evaluation value and cannot be a neutral (Ossowska 1963: 11). However, not every behavior is subject to such an assessment, because it can be axiologically neutral in itself. The context dispels doubts here. For example, taking a seat on the bus while traveling to work, as behavior without a specific context will be considered as morally neutral. In contrast would be the theft of money from a homeless beggar. However, occupying a seat in a bus in the presence of a standing elderly person or a pregnant woman with two small children can already be judged negatively in moral terms. The assessment also depends on the rigidity level – form principled to situational ethics (Lazari-Pawłowska 1992b: 43). As it was mentioned in the beginning of the article, many researchers try to describe hackers' culture and grand rules which are important for them, but the most advanced and complex is Steven Levy's approach (2010: 28-31). He points out that the hackers' ethics consist of these six rules: 1/ Access to computers – and anything that might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On Imperative! Levy starts his considerations by stating that hackers fight about information limitation in any sense (cf. 2nd point), but this point refers specially to access to computer. In that vision everyone should have access to computers[1], and should not be limited by the lack of knowledge how to use a such device. They resent any person, physical barrier or law that tries to keep them from doing this. In this conviction we can find the universal desire for all humankind to make people's lives easier and more convenient. This looks like not only a concern for hackers' interests (like making computers more popular and finding access to crack security boundaries and steal information) but it is somehow a fight against social differentiation. In this "utopian" vision every human has the ability (knowledge, possibility) to use computer devices and make life easier and happier. This part of the hackers' moral code shows concern for everyone, what obviously can be used in non-ethical ways because the hackers' group is not homogeneous. 2/ All information should be free. In this point Levy refers to unlimited access to all information. This approach raises a number of problems. First is privacy. Can people hide some data and decide what amount and to whom to show them? What about personal data, family photos, medical information about diseases – should they also be published? Privacy needs seems to be natural and connected with decisions about what, where and when could something be made public. Levy does not specify this, but it seems that hackers' preference was not to make public every single piece of life, but rather to ensure information transparency. Access to information is unlimited, which means that there are no divisions, but everyone has the ability to view information. This means limpidity of already published information. Users should not have to pay for it. Everyone can use data and be aware of them. This refers especially to source code of application and prevents "(...) the dreaded, time-wasting ritual of reinventing the wheel: instead of everybody writing his own version of the same program, the best version would be available to everyone, and everyone would be free to delve into the code and improve on that" (Levy 2010: 29). This vision spread in the open access philosophy. 3/ Mistrust Authority – Promote Decentralization. Levy points out that in the hackers' perspective bureaucracy is not helpful in the information spreading process. When developers want to share a project code, they expect commitment in reviewing it, fixing bugs, and requesting for some changes. This can be done when other users are unbounded and free to join the project. The great example of such an approach is open source software, which is the software where source code can be inspected, modified and enhanced by anyone (opensource.com 2018). The last thing the user needs is bureaucracy present in big corporations, government or educational institutions, which hides behind arbitrary rules, rigid processes, dehumanized ordinances to which computer users must follow and adjust. In place of this hackers' environment is propose decentralization and lack of central authority above themselves. 4/ Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position. In that case hacker's society wants to be treated as valuable and evaluated using substantive criteria. This means that neither social roots, educational level, years of experience should not be taken into consideration, because they are not the point here. The aim of accomplishment or bad behavior should be judged *per se* based only on technical, law and ethical criteria. Depending on what was done and what were the social consequences, this action should be evaluated somehow. If it harms someone's interest and breaks the law, then this act should be punished according to its evaluation. On the other hand, extending a bit Levy's description, if hacking has got bigger positive influence than negative, it should be somehow "rewarded" – even if it is illegal! – but to help humanity in the utilitarian manner. This statement may introduce lots of confusion, but on the background of each "hacking tools" usage there is a clause that the usage is limited to test purposes, like Kali-Linux for security penetration testing for instance (Halton, Weaver 2016: 16). Under the hood there is always a contract. According to *Certified Ethical Hacker v9* guide-book "a contract is essential for another extremely important reason as well: proof. Without a contract you have no real proof that you have permission from the system owner to perform any tests" (Oriyano 2016: 60). 5/ You can create art and beauty on a computer. In that sense the beauty of the program code by itself and its openness to be shared with the whole Internet society brings value. Everyone could adore the beauty of the source code, comment on it and improve it. This aesthetic elevation was compared by S. Levy to mu-

[1] According to von Neumann's architecture, machine (in that sense 'computer') "(...) is a design model for a stored-program digital computer that uses a processing unit and a single separate storage structure to hold both instructions and data" (computinghistory.org.uk 2018). Today a lot of devices fulfill those criteria – not only personal computers or laptops, but also cell phones (smartphones) which now are super small but really powerful.

sic’s beauty, harmony and perfection (in that case of Johann Sebastian Bach’s *Rest in Peace*) (Levy 2010: 34). 6/ Computers can change your life for the better. Hackers claims that surely computers are changing people’s lives, enriching them and making them more adventurous. Everyone could benefit from experiencing this computer power. Surely everyone could benefit from a world based on the Hacker Ethic, where a world opened up by the computer is a limitless one (Levy 2010: 34-35). 7/ Levy’s rules are more general than corresponding to specific cases. Described above, the hackers’ moral code sounds to be an idealistic vision, but fully compatible with open software approach and Linux philosophy (cf. Chmielecki 2014: 197-198). Levy’s characteristics could be extended by diversified assessment to psychological, social and system manner (Lazari-Pawłowska 1992a: 99-101). According to this distinction, hackers’ acts could be classified as “moral” on each of those layers separately. One should take into consideration the wider context of the act, the motives behind it and a hacker classification to a particular group. It may be somewhat questionable to consider motivation for reasons of higher good, which would justify a given offense. In some cases, breaking the security boundaries of computer software could help lots of people in the utilitarian manner – to avoid troubles or wrongly invested money. The perfect example is the pen-testing procedure which is common in software companies. Testing the security limitations, breaking the working application or physically destroying the infrastructure may reveal the weaknesses and strengths of tested IT solutions and then help to improve it and be prepared for the next potential attack.

Do hackers need and follow ethics?

The answer for this question depends on separate cases. However, the existence of a so-called hackers’ code of ethics does not mean that everyone from hackers’ society follows it. This set of principles is not an internalized moral code, but rather a few ideas with more or less agreement among hackers. Available IT tools can be used in a different way and to meet different expectations. Let’s examine the before mentioned Kali-Linux. It can be used to prepare penetration tests to find out an application’s (or entire software ecosystem’s) security holes and vulnerabilities during the network attack. In a different scenario, it can be an attempt to steal the personal and sensitive data and prepare some unauthorized transactions from a user bank account. In this second case, the usage of Kali-Linux software is not ethical and is banned by the application vendor. However, this limitation does not block, in any way, the improper usage and breaking the law. The factor which decides about the ethical or non-ethical usage is personal morality (and existence of rudiments of some code of ethics – no matter if written down or only conceptual, personal or accepted by wider audience). The hacker’s intention exactly is the factor which differentiates “white hat” and “black hat” hackers (Lockhart 2007: XV). The third separate approach is security auditing which involves comparing a company’s security policies (or compliance requirements) to what is actually taking place (Beaver 2016: 12). No matter what, users need to be aware that their decisions, acts, and responses are nowadays visible to everybody. Everything is transparent, even if the user decides not to put this content on the Internet. Obviously, someone else can do this without the user’s permission. That’s the brutal reality. In the 21st century there is no such thing like “anonymity” or “privacy”. People are trying to hide their personal details (i.e. IP address) somewhere behind a VPN, Proxy Server, or TOR but sooner or later their identity comes to light (quora.com 2018). Sometimes that information could be used to improve security by government authorities for public safety reasons, but sometimes by non-authorized groups for unknown purposes. Transparency of information is on the one hand, one of the general hackers’ basic rules, but on the other hand especially hackers cherish their anonymity – that’s the hackers’ paradox. This turns to consideration – do hackers’ still need some grand rules of moral behavior if they cannot meet their own grand rule of unlimited access to information? The general answer assumes to be positive, but it still depends on individual motivation and being identified as a “white-” or “black hats”. The hackers’ society was founded on a few basic principles, that are still valuable and worth pursuing. Although it is not possible to meet them fully, those ideas are universal and cross-national and could be internalized by hackers from all over the world.

Bibliography:

1. Beaver K., (2016) *Hacking for Dummies*, 5th Edition, New Jersey: Wiley.
2. Chmielecki P., (2014) *Linux Myth. Open Source Society in Information Society* [w:] Filipovic I., Klacmer Calopa M., Galetic F., (red.), Economic and Social Development.
3. Halton W., Weaver B., (2016) *Kali Linux 2: Windows Penetration Testing*, Birmingham-Mumbai: Packt Publishing.
4. http://www.businessdictionary.com/definition/hacker.html [29.12.2018].
5. http://www.computinghistory.org.uk/det/3665/john-von-neumann/ [29.12.2018].
6. https://en.oxforddictionaries.com/definition/hacker [29.12.2018].
7. https://opensource.com/resources/what-open-source [29.12.2018].
8. https://www.merriam-webster.com/dictionary/hacker [29.12.2018].
9. https://www.quora.com/Why-TOR-is-not-secure-anymore [29.12.2018].
10. https://www.urbandictionary.com/define.php?term=hacker [29.12.2018].
11. Kołakowski L., (1978) *Main Currents of Marxism*, Warsaw: PWN.
12. Kołakowski L., (2009) *Etyka bez kodeksu* [w:] Kołakowski L., Kultura i fetysze, Warszawa: PWN.
13. Lazari-Pawłowska I., (1992) *O pojęciu moralności* [w:] Lazari-Pawłowska, Etyka. Pisma wybrane. Wrocław-Warszawa-Kraków: ZN im. Ossolińskich.
14. Lazari-Pawłowska I., (1992) *Problemy etyki sytuacyjnej* [w:] Lazari-Pawłowska, Etyka. Pisma wybrane. Wrocław-Warszawa-Kraków: ZN im. Ossolińskich.
15. Levy S., (2010) *Hackers: Heroes of the Computer Revolution*, Beijing-Cambridge-Farnham-Köln-Sebastopol-Taipei-Tokyo: O’Reilly.
16. Lockhart A., (2007) *Network Security Hacks*, 2nd Edition, Sebastopol: O’Reilly.
17. Oriyano S.P., (2016) *Certified Ethical Hacker Version 9 Study Guide*, Indianapolis: Wiley.
18. Ossowska M., (1963) *Podstawy nauki o moralności*, Warszawa: PWN.

O Autorze

dr inż. Przemysław Chmielecki

0000-0002-4471-4158

Adiunkt w Zakładzie Filozofii w Katedrze Teologii Systematycznej Wyższego Baptystycznego Seminarium Teologicznego w Warszawie. Doktor filozofii (specjalizacja w obszarze filozofii nauki), magister inżynier informatyki (programowanie), magister kognitywistyki i resocjalizacji. Wcześniej związany również z socjologią i obszarem badań empirycznych jako współpracownik największych krajowych instytutów badawczych (IPSOS, Millward-Brown, TNS, PBS). Od kilku lat pracuje jako specjalista IT w obszarze chmur obliczeniowych i zarządzania dużymi instalacjami serwerowymi.