Int J Ethics Soc 2024; 6(2): 9-19

10.22034/ijethics.6.2.9

INTERNATIONAL JOURNAL OF Ethics & Society

Review Article

Explaining the Hacking of Society's Information Systems from the Point of View of Ethical Theories

Noah Zhang[1*], Liam Wang[1], Isla Wilson[2]

1. Department of Computer Science, Faculty of Engineering, University of Canterbury, New Zealand.
2. Department of Computer Science, Faculty of Computing and Mathematical Sciences, University of Waikato, New Zealand.

Corresponding Author: Noah Zhang, Department of Computer Science, Faculty of Computing and Mathematical Sciences, University of Waikato, New Zealand. E-mail: zhang.noah@gmail.com

Received 25 Apr 2024 **Accepted** 18 May 2024 **Online Published** 26 Jul 2024

Abstract

Introduction: One of the important topics in the field of information technology is hacking the information systems of societies, that is, finding the security weaknesses of a system to penetrate and access its information. which can be done with various motivations, such as measuring penetration, finding system flaws, curiosity, causing disturbance, breaking the security of systems and harming them, personal gain, and so on. Hacking information systems will have favorable or unfavorable consequences for communities and citizens. Therefore, the purpose of this research is to explain the validity or moral impropriety of this act based on three important moral theories of consequentialism, deontologism, and virtuism.
Material and Methods: This research was carried out using a descriptive analytical method based on library sources.
Conclusion: Based on the results of the present study, it can be said: from the point of view of utilitarianism, the greater the amount of social benefit from the action of the influencers, the more ethical their action is, and the more harmful it is to the society, the more unethical their action is. Ethical values such as trustworthiness, not prying into the privacy of others, not harming people, maintaining human dignity, protecting public interests, are among the ethical rules governing the act of hacking. And the benevolent motives of hackers only when they are compatible with these moral rules, is the moral justification of their action from the perspective of rule-oriented duty-bearers. The specific personal, social, cultural and economic conditions of the hacker are effective in the moral judgment of his actions from the perspective of practical duty-oriented people. In the end, it should be said: Knowing the ethical behavior of hackers and its effect on their actions is the main condition for the ethical evaluation of information systems hacking, although it will be very difficult to achieve such knowledge.
Keywords: *Hacking, Ethics, Information Systems, Society*

How to Cite: Zhang N, Wang L, Wilson I. Explaining the hacking of society's information systems from the point of view of ethical theories, Int J Ethics Soc. 2024;6(2):9-19. doi: 10.22034/ijethics.6.2.9

INTRODUCTION

One of the capabilities of cyberspace is the possibility of hacking information systems. By creating challenges in "privacy" and "property", this has faced the society with various economic, security, cultural and similar problems. According to a study by HP in 2015, the economic damages caused by the hacking of information systems in various countries such as the United States, England, Germany, Australia, Japan, Russia, and Brazil have been increasing due to the increase in the number and intensity of hacking attacks. These attacks include: stealing the intellectual property rights of companies and organizations, confiscating online bank accounts, creating and spreading viruses on other

computers, publishing confidential business information on the Internet, and disrupting the vital and national infrastructure of the target country (1, 2).

Due to the various consequences of activities in cyberspace, the concept of ethics in cyberspace, followed by "hacking ethics", has been the focus of various social groups for several decades. And to protect users from unethical behavior, dos and don'ts have been predicted at the international level. This has led to the emergence of a new concept in the literature of professional ethics called "ethical hacking (ethical hacking)" and based on it, hackers are classified into two groups: "good hacker" and "bad hacker". Since the act of hacking is done by people with different motivations and different consequences, and it has different consequences, it seems necessary to evaluate the act of hacking on three important moral normative theories; consequentialism, deontologism and virtuism. Also, its validity or invalidity should be explained.

MATERIAL AND METHODS

Therefore, the present research, which was carried out by descriptive-analytical method and using library resources, lacks an effective background.

DISCUSSION

Concept of hacking

The meaning of "hacking" is to find the security weaknesses of a system in order to penetrate it; without having permission to access that system (3). There are two meanings for the word hacker. In the beginning, a hacker was "a curious programmer who is interested in manipulating and improving software and electronic systems and enjoys discovering and learning how computer systems work" (4); "He is someone who enjoys delving into the details of programmable systems and is determined to beat the computing capabilities of a machine against his human intelligence. A person who is persistently and stubbornly obsessed with programming. The intruder is not malicious and does not harm" (5). Accordingly, a hacker is a person who has great talent in expanding the work and performance of computers as well as their original design, and acts as a curious and honorable person (6); But in recent years, the term hacker has been used in a new sense and it means "a person who, with the wrong motivation, hacks information systems and implements his malicious goals by infiltrating computer systems" (4). In this definition, hacker is used synonymously with the word "cracker".

Literature of hacking

The term "hacker" was used for the first time in the 1960s at MIT University. (5). The first generation of hackers were interested in acquiring high-level technical skills, for this purpose they had undeveloped ethical standards. According to Steven Levy, the ethical code of hackers was a philosophy of sharing, free-thinking, decentralization and real-time access to computers to improve them and improve the world. From the beginning of the formation of the second generation of hackers, a clear relationship between counterculture and cyber culture can be seen; Because the ethical standards of hackers, which was on the one hand non-political and focused on technical issues, and on the other hand, is destructive and completely ideological, which was not very effective. In the mid-1960s, computers replaced human operators or rudimentary electromagnetic systems in telephone companies, opening up a new digital world to hackers. The third generation of hackers, who are telephone hackers, quickly realized the potential of telephone systems and long-distance telephone lines by simulating the systems' in-band signals. Although this act was considered theft from the point of view of telephone companies; But the hackers considered their

actions illegal only if they violated AT&T's privacy (7).

In the early 1980s, after the spread of digital networks, the "414 S" group was the first group to be noticed by the security services. This group consisted of a number of high school hackers in Milwaukee, USA, who broke into the computers of the American Cancer Center and the Los Alamos National Library. This event, together with the movie "War Games", made the public think about the question of how to protect the information stored in computers? Because every person owned one of the popular microcomputers of the time and had the capacity to unlock the secrets contained in the computers used in banks, hospitals, companies and even military installations. In these years, events such as the exploding gas pipeline of the former Soviet Union in 1982 were carried out by the CIA and with soft manipulation (7).

In the late 1980s, hacktivism (infiltration) movement tended towards anti-security and anti-human activities, and therefore, whenever the word hacker was mentioned in the news media, the image of a computer thief or an evil vandal was visualized in the audience's mind; This mentality was incompatible with the background and culture of influence that originally belonged to the elite of computer-related fields. Hackers considered this a great insult to this group of experts. This caused those who used to be proud of the title of "hacker" to be extremely unhappy. Hackers tried to demarcate themselves from saboteurs through definition and vocabulary, showing that the hacker is a positive and elite human being who is opposed to "crackers". From their point of view, crackers are worthless and sick people who, through learning some hacking skills, do worthless things like stealing usernames and passwords of others, harassment and illegal and unethical operations. And by breaking the privacy of a system, they pursue their dishonest goals (5).

Types of hacking

Hacking is divided into ethical hacking and unethical hacking based on the validity of following or not following ethical rules:

Ethical hacking includes methodical and legal penetration testing, white hat hacking and vulnerability testing. Ethical hacking is the use of common tools and methods for hacking with the permission and knowledge of the target organization or network and in a professional environment. The purpose of this hack is to discover vulnerabilities from the point of view of a malicious attacker in order to increase the security of the system. In other words, ethical hacking is a part of an overall information risk management program and causes smoothing and continuous improvement; It also helps to ensure the correctness or falsity of suppliers' claims about the security of their products (4). Every ethical hacker must follow a few basic rules to ensure that his hacking is ethical in order to achieve positive results: Not misusing information, respecting the privacy of others, not harming systems, using ethical hacking process, getting legal permission to hack, choosing the right tools, ensuring that the right tools are used (by testing the tools), implementing the ethical hacking program confidentially and evaluating the results (4).

Unethical hacking is exploiting users and deceiving them based on social engineering to obtain information for nefarious purposes. Also, common and effective physical attacks against information systems (unauthorized entry of hackers into buildings, computer rooms, and other places where sensitive information and assets of users are located) and theft of computers and other valuable equipment are examples of unethical hacking (4).

Types of hackers

There are different types of hackers with different credentials. One of the most widely used

classifications is the division of hackers based on their hat color; Because for them white, black, gray, blue, red, yellow, pink, green and purple hats are considered depending on the purpose and consequences of their activities, the most common of which in the world hacking literature are white hat, black hat and gray hat hackers.

White hat hackers (good hackers): This group is elite people whose activities are not harmful; they cause the structure and dynamics of information systems. Good hackers, without bad motives, try to break the security of systems and reveal their weaknesses in the face of sick or biased intruders (penetration testing). White hat hackers adhere to the principles of "ethical hacking" and usually have a high level of knowledge and experience. "Principled hackers" is the title that is given to them due to having an ethical mission. The ethical principles of this mission: not harming the system, not infiltrating government or security networks that are engaged in national duty; Not tampering with system files and transferring them; Not leaving a trace in the compromised system; Not giving information and knowledge to other people about your knowledge and hacking skills (except to experts and trusted people to improve specialized skills and exchange ideas); Not sharing information on the Internet about your hacker details; Failure to break into a system a second time; Being creative and presenting a new method (at least for once) (5).

Black hat hackers (intentional and malicious hackers): These people hack information systems only for personal gain or unethical intentions, compared to white hat hackers; However, in many cases, the mistakes of users lead to the penetration of these hackers. For example, choosing the year of birth or phone number as a password is a factor for black hat hackers to penetrate people's systems. These hackers are trying to destroy computer systems and discover the information of their users by using the method of creating and sending a malware (virus). The golden age of black hat hackers was the 1980s when computer systems were newly developed; But today, no one can earn an acceptable income in this way, and due to the development of security systems, these people are arrested and have serious social problems (4). Users have different types of thinking; Some are very good at their work; Some also try to penetrate without mastery and skill in the field of information technology of an organization (5).

Gray hat hackers (slightly good and slightly bad hackers): Due to the gray combination of black and white, a gray hat hacker is a hacker who has some characteristics of both white hat and black hat hackers. Some hackers try to hack information systems by checking the security status of sites and servers and with the motivation of learning or curiosity. These hackers, known as "walkers", steal their information without harming the target systems. Gray hat hackers have a lower level of knowledge and information than white hat hackers and enter other people's systems without permission; Also, they cause less damage to the system than black hat hackers (4, 8).

Hacking information systems of societies from the perspective of ethical theories

A) Moral theory

If we define "theory" as "a set of propositions responsible for the rational explanation of the relationships between the concepts in the set of these propositions"; Then the moral theory is "a set of non-contradictory propositions that are responsible for the rational explanation of the existing relationships between moral concepts, and have the ability to falsify their hypotheses" (9).

Ethical theories can be divided into different types according to the criterion they provide for determining good and bad, among which the three theories of "consequentialism", "deontalism" and "virtuism" are more important.

These three approaches are divided into two They give a clear answer to the main question: What is ethical to do in any situation? What should be done when moral conflicts arise? (10).

Consequentialist moral theory: every action that a human does has an effect on the universe; Sometimes the remains of an act are not very important; Like prioritizing wearing shoes on the right foot instead of the left foot, sometimes these works have great importance for the individual or the society; both in the positive and negative aspects; such as choosing a person to marry instead of another person or abortion (11). In consequentialism, what is considered to evaluate a behavior is the consequence of that behavior. The amount of good and evil that comes from doing an action is effective in whether it is good or bad. If the relative good created by performing an action is more dominant than its evil, it is considered a factor of moral judgment and judgment regarding that action; But if the act done has worse than its good, it will be considered as an evil and wrong act in the judgment; Because human actions in most cases are not always the result of pure good or pure evil, they bring both results. Important in the conclusion, the degree of victory of evil over good or good over evil has been done in practice (9). In the theory of consequentialism, something outside of ethics is effective in describing moral or immoral behavior; Therefore, what is meant by "good" and "evil" is not a moral matter that avoids problems and interprets good with good and bad with bad; Rather, there is another criterion here to measure the goodness or badness of the action (12). According to some philosophers, this criterion (external matter) is the pleasure and pain caused by the action (hedonism), that is, an action is right if, at least compared to its alternative, the pleasure prevails over the pain (9, 12); But according to Jeremy Bentham (1832-1748 AD) and his student John Stuart Mill (1873-1806 AD), this criterion is the profit from the action (utilitarianism) (13).

Jeremy Bentham, who is the founder of the theory of act- utilitarianism, equates good with happiness and happiness with pleasure, and considers public benefit as a means to achieve personal benefit. He believes that any action that increases public benefit will also increase personal benefit, and conversely, the greater the public loss, the greater the personal loss (13-15). According to John Stuart Mill and his followers (rule- utilitarianism), collective benefit is important; Therefore, contrary to the theory of act-utilitarianism, in which originality is with personal pleasure and profit, in this theory, originality is with collective profit (16). In this case, unlike act-utilitarianism, here we can provide a general moral rule for all people who are in the same situation.

According to Bentham, to calculate this pleasure and preference between actions that have two aspects of good and evil, seven directions should be considered. The greater the intensity, stability, certainty, closeness, fertility, purity and extent of the pleasure of an action, the preference is with that action (12, 17). In other words, the degree of desirability of each pleasure is obtained by calculating a special coefficient determined for these seven criteria. Of course, the results of previous calculations can also be used to determine the moral duty (18).

Deontological ethics theory: In the deontology theory, the action itself is important regardless of the consequences that result from it. From the point of view of deontologists, in addition to the consequences of a good or bad action, other considerations such as the compatibility or inconsistency of the performed action with the duty that exists for the actor are also taken into consideration; In such a way that harmony with duty can make the voluntary action of a person morally obligatory (12).

Deontology theories are divided into at least two general types: act-deontologism and rule-deontologism. In the theory of act-deontology, the moral duty of humans is determined case by case, and it is not such that, for example, it is possible to provide a general law that "everywhere one should make truthfulness one's profession" or "lying is bad in all cases"; Rather, the position of individuals plays the main role here and the unique conditions of each person have their own ruling (9).

In rule-deontology, which "Immanuel Kant" played an essential role in its growth and development, the criterion for distinguishing right from wrong action is not the rules obtained from the results of minor cases; Rather, it is these general rules that are the standard of moral behavior and the rulings of specific cases are determined in the light of these rules (12). According to Kant, none of the "mental abilities" such as intelligence; "Secretary characteristics" such as courage, diligence and perseverance; "Blessings of fortune" such as power, wealth, honor and "happiness" are not intrinsic and absolute good; Because all these things can create conditions that are morally worse; Like a criminal who is smart or a powerful and rich person who has committed a heavier and bigger crime due to having this power and wealth (17); Therefore, according to Kant, being good is determined by having a "good will" and a person who lacks such a will cannot be a good person (19). Of course, the meaning of this good will is not that it reaches satisfactory results; Because the act of a criminal who has a bad motive may also lead to good results; Rather, this being good is due to the good will itself, and this will is realized when it is due to the fulfillment of duties and obligations; That is, a person is good when he does work with the motivation of doing duty, not because of a feeling of pleasure or a feeling of kindness or generosity (19).

Ethical virtuism theory: Socrates, Plato and Aristotle can be mentioned as the most important proponents of this theory. Virtue refers to the characteristics that lead to human superiority or magnanimity; Whether it is natural characteristics such as strength and intelligence or acquired characteristics such as skill or internal characteristics such as cheerfulness and courage (11). One of the differences between the virtue theory and the previous two theories is that the ethicist tries to determine the path to happiness by teaching good behavior to people and shows the way to avoid it by showing bad behavior. In this case, these virtues are the moral guide for the individual in the position of action; Contrary to the deontology theory, virtue is not a moral guide in the position of action, and general principles and rules guide people, which if believed in those principles only guarantee the performance of action in special situations and with passion and desire and in accordance with the principles (12).

B) Ethical analysis of hacking

Ethical explanation of hacking in consequentialism: To prove the validity or wrongness of hacking based on consequentialism, the consequences of hacking must first be examined. Although about the consequences of hacking, no independent research has been done so far; But the consequences of using virtual space (Internet) and using computer technology can be enumerated in some cases by generalizing the consequences of hacking (20). Based on this, the consequences of hacking and being hacked can be divided into two forms of positive and negative consequences, as follows. The consequences of hacking can be divided into two types of positive and negative consequences. First, the desired consequences: Some of the desired consequences of hacking are: acquiring prevention and coping skills (preventing intruders from attacking people's systems and, as a result, preventing the

disclosure of their information); Business opportunity development (employing people in security and information centers and making money from discovering vulnerabilities and network problems, providing solutions for them); Improving the security level of systems (hacking the system causes awareness of its disadvantages, increases the scope for improving the security level of that system); exposing the actions of intelligence and security services (when the security of the society is endangered, by using hacking, it is possible to find out about the malicious intentions of people who intend to do such a thing and take the necessary measures to face it); Increasing the security factor of users (by identifying ways of penetration and creating a dedicated and strong firewall, the security factor of users increases when using computers and new technologies); Development of computer-related technologies (finding out the vulnerable points of systems and electronic devices in order to create and use impenetrable methods and tools); Prevention of social disturbances (cyber-attacks and creating problems in the financial and economic system are among the disturbances that can cause irreparable damages; awareness of these types of attacks is effective in preventing and preparing to face them); Get the latest news (access to confidential and classified news that endangers national security). Second, the adverse consequences of hacking Some of the most important adverse consequences of hacking are: violation of dignity and violation of privacy (despite many rational and narrative recommendations on preserving dignity and respecting people's privacy (21). By logging into a personal account and accessing people's private information and violating their privacy, hackers provide the basis for insulting their dignity and reputation); Creation and development of mental injuries (revealing crimes and the dangers caused by them causes the spread of anxiety and a sense of insecurity among users) (22); The spread of moral corruption (access to immoral content and its public distribution leads to normalization, increasing norm-breaking and promotion of moral vices in the society); Creating a sense of insecurity regarding the functioning of computer systems and electronic devices (accessing and controlling cars with Wi-Fi, Bluetooth and GPS systems, mobile phones, printers connected to the Internet, digital cameras, energy meters, Internet phones, and the like, causing a sense of insecurity in users) (23, 24); Disturbance in social relationships and interactions (people who are subjected to psychological, emotional and bullying abuse are more vulnerable to isolation and social aversion than others) (25, 26). This is also true for the people whose information is hacked, the hacking victim's feeling of being blackmailed by the hackers in order not to publish their information provides the basis for this damage). negative growth of technology development (not using new technologies due to the lack of trust in them, prevents efforts to recognize their technical weaknesses and build new technologies); The spread of crime (access to confidential information of individuals and organizations is one of the important factors for creating or intensifying the feeling of revenge in the victims, it creates a platform for the occurrence of crime in the society) (27); spreading the culture of earning illegal income; The dominance of aliens and enemies over information (the disclosure of classified information of organizations and targeted planning to destroy their scientific and technical infrastructure) (28); Endangering the material and intellectual rights of organizations, companies, social groups, and individuals (access to the confidential information of organizations and companies, while threatening the initiative of human resources, hinders the development of research, science, technology, and trade, and also results in great economic losses) ; Promoting modern addictions (addiction to hacking without

proper motivation and only for fun is one of the examples of modern addiction) (29).

Since in rule-oriented utilitarianism, originality is with collective benefit, if the act of hacking has collective benefit, it can be recognized as a moral act. Based on this, if the result of the infiltrator's action is to reveal the intentions of the enemy, thieves, and the like, it is considered a good action; even if it is not done using the correct methods and the hacker did not start such an action with a positive intention at first (black hat hackers); However, if the hacker hacks with good intentions, but the result is the disclosure of the country's or government's secrets or causes the hacked person to be insulted, because the harm of this act is greater than the good, it is considered an improper act. As a result, it is not possible to consider the actions of white hat hackers as legitimate and the actions of black and gray hat hackers as illegal; Because in this ethical system, the intention and motivation of hackers do not play a fundamental role in the moral judgment of their actions, and it is important that the consequences of the hacking act are aligned with the amount of collective profit. Based on this, the ethical rule of "respecting people's privacy" or "improperly spying on other people's affairs" in conflict with national security or public interest, is set aside, the rule of "maintaining the maximum interests of the society" will be the criterion of action.

In act- utilitarianism, good is equivalent to happiness and happiness is equivalent to pleasure. But because personal pleasure is meant, the action of hackers in whatever color of hat they are, especially pink hat or green hat hackers who do this for their own fun and personal pleasure, is an ethical thing. If the hacker realizes a pleasure with his action that overcomes his pain, his work is recognized as right and "morally good".

Due to the wide range of positive and negative consequences, it is not possible to make the same judgment regarding the legitimacy or impropriety of hacking in this device, and this makes it difficult to make a decision on how to deal with it. This point is more prominent for gray hat hackers than other hackers. To justify the ethical nature of their work, these hackers point to general and unclear concepts such as the authenticity of freedom of information, providing public service in order to increase information security, using unused resources, and protecting society, which are not easy to prove in all cases (2).

As mentioned before, Bentham considered the seven components of intensity, stability, certainty, closeness, fertility, purity, and extent of pleasure to calculate current pleasure and preference, which has two aspects of good and evil (12, 17). Based on this, the ethical audit of hacking in pragmatic utilitarianism is dependent on the degree of intensity, certainty, proximity, fertility, purity, and extent of the pleasure (profit) in the act of hacking; Without there being any difference between the types of hackers. As a result, without a general rule to evaluate hackers' actions, each hacker's action will be measured according to his own conditions, there will be a moral judgment based on the number of people who infiltrated.

Ethical explanation of hacking in deontologism: the influencer's behavior in rule-deontologist orientation is measured by his motivation. White hat hackers (lawful hackers) solve security problems at different organizational, national and global levels by having technical skills. The motivation of these hackers is to neutralize cyber-attacks leading to extortion, fraud and the like (5). Therefore, the action of white hat hackers is moral, even if it does not lead to public benefit and does not lead to the greatest victory of good over evil for the person, society or the world. Maybe their actions will lead to the disclosure of secrets and loss of cyber security. Black hat hackers, hacktivists, money hackers and cyber terrorists, although they function like white hat

hackers; But because they do hack with unhealthy competitive motives, incorrect political goals, terrorist goals, disrupting public order, illegal acquisition of wealth, stealing information, harassing and gaining fame, their action is unethical; Although the public benefit resulting from their actions is more than the actions of white hat hackers (5). In many cases, the goal of gray hat hackers is humane, although they sometimes use unethical means to achieve it. These hackers consider their work to be ethical and believe that they are doing their duty, i.e. preventing the possible abuse of users' systems (2). Since in the duty-oriented ethical system, the motivation of the actor in acting is the duty that distinguishes the moral action from the unethical action, three basic questions must be answered:

First: What is the ethical deontology of the activist in hacking? Trustworthiness, not prying into the privacy of others, not harming people, maintaining human dignity, protecting public interests, are among the ethical duties related to hacking. Therefore, hackers' benevolent motivations are moral justifications of their actions only if they are compatible with their moral duties.

Second: In the conflict between moral duties, which duty comes first? For example, if there is a conflict between the duty to protect the public interest or national security and the duty to protect the privacy of individuals, the duty that is more binding, i.e. the duty to protect national security, is preferred. Thus, the ethical rule governing the act of hacking information systems should be explained as follows: Respecting people's privacy is ethical only when national security or public interest is not endangered.

Third: What is the authority of task recognition and preference? The customary moral intuitions of the society in the position of action can judge the type of duty and the preference of one of them in the position of conflict. Whatever reason and custom deem more important, it has more obligation and is preferred over the duty in front of it (9).

But based on the attitude of act-deontology, it is impossible to answer the question of whether hacking is morally permissible or illegal, and a general judgment cannot be issued regarding it; Rather, it should be asked whether the act of hacking issued by person "A" is ethical or unethical according to his specific personal, cultural, social and economic conditions. It is natural that the sentence issued to this person is not a general sentence applicable to all cases; Because the position of people plays a fundamental role in the moral judgment of their actions, and every situation is unique and unique; Therefore, the placement of a hacker in any group of hackers cannot alone lead to the moral judgment of his action.

Ethical explanation of hacking in Virtuism: According to Virtuists, the moral examination of an action is dependent on knowing the inner character of the person who tried to do it; Because the behavior of the activists comes from their inner traits. Based on this, in the ethical analysis of the act of hacking, it is necessary to determine that the intruder's act of infiltrating the information systems of real or legal persons is the result of the effect of which of their internal traits and characteristics. To realize such an analysis, it is not always useful to pay attention to the classification of hackers, because in this classification, less attention is paid to the internal behavior of the infiltrators, the basis of which is more the consequence of their actions. In any case, if the act of hacking stems from vices such as "revenge", "jealousy", "spying", "maliciousness", "harassment", hacking other people's information systems is reprehensible and immoral; But if doing this act on the part of the intruder comes from virtues such as "benevolence", "justice", "altruism", infiltrating other people's information systems will be a desirable and ethical thing.

CONCLUSION

System hacking refers to the use of technical skills and knowledge to gain access to a computer system or network. Hackers use many methods to break into a system by exploiting vulnerabilities and disguising their activities to avoid detection. The results of the present study showed that:

The greater the amount of social benefit resulting from the actions of hackers, regardless of what motivation they have for hacking information systems in societies, the more ethical their actions are from the perspective of rule-consequentialists. And on the other hand, the more harmful it is to the society, the more unethical their actions are. Ethical values such as trustworthiness, not prying into the privacy of others, not harming people, maintaining human dignity, protecting public interests, are among the ethical rules governing the act of hacking. And the benevolent motivations of hackers only if they are compatible with these moral rules, is the moral justification of their action from the point of view of rule-deontologists. The specific personal, social, cultural and economic conditions of the influencer are effective in the moral judgment of his action from the point of view of act-deontologist, it is not possible to morally evaluate their action based on the common classification (white, black and gray). In the end, it should be said: knowing the ethical behavior of hackers and its effect on their actions is the main condition for the ethical evaluation of intrusion into information systems in the ethical apparatus of virtue, although it will be very difficult to achieve such knowledge.

ETHICAL CONSIDERATIONS

Ethical issues (such as plagiarism, conscious satisfaction, misleading, making and or forging data, publishing or sending to two places, redundancy and etc.) have been fully considered by the writers.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interests.

REFERENCES

1. Segers R, Erp M, Meij L, et al. Hacking history via event extraction. Proceedings of the 6th International Conference on Knowledge Capture (K-CAP 2011). Alberta, Canada. 2011. 10.1145/1999676.1999705
2. Yamaneh S. Understanding Hackers and the Historical Development. Ieice Ess Fundamentals Review 9(3):197-204. Doi: 10.1587/essfr.9.3_197
3. Cekerevac Z, Dvorak Z, Prigoda L, Cekerevac P. Hacking, protection and the consequences of hacking. Communications - Scientific Letters of the University of Zilina, 2018; 20: 83-87. Doi: 10.26552/com.C.2018.2.83-87
4. Alhamed M, Rahman MM. A systematic literature review on penetration testing in networks: future research directions. *Appl. Sci.* 2023; *13*(12). Doi: https://doi.org/10.3390/app13126986
5. Lubke J, Britt VG, Paulus TM, Atkins DP. Hacking the literature review: opportunities and innovations to improve the research process. Reference & User Services Quarterly; Chicago, 2017; 56(4): 285-295.
6. Shaqiri A. Management information system and decision making. Academic Journal of Interdisciplinary Studies, 2014; 3 (2): 18. Doi: 10.5901/ajis. 2014.v3n2p19
7. Al-fuhaidi B, Al-Sorori W, Maqtary N, Al-Hashedi A H, Al-Taweel S. Literature review on cyber-attacks detection and prevention schemes. International Conference on Intelligent Technology, System and Service for Internet of Everything (ITSS-IoE). Sana'a, Yemen. 2021.
8. Chng S, Lu H, Kumar A, Yau D. Hacker types, motivations and strategies: A comprehensive framework. Computers in Human Behavior Reports, 2022; 5(2): 100167. Doi: 10.1016/j.chbr.2022.100167
9. George T, Oliver B, Gregory L. Issues of implied trust in ethical hacking, The Orbit Journal, 2018; 2(1): 1-19. Doi: https://doi.org/10.29297/orbit.v2i1.77
10. Caldwell T. Ethical hackers: putting on the white hat. Network Security, 2011; 2011(7): 10-13. Doi: https://doi.org/10.1016/S1353-4858(11)70075-7
11. Yaokumah W. Predicting and explaining cyber ethics with ethical theories. International Journal of Cyber Warfare and Terrorism (IJCWT), 2020; 10: 46-63. Doi: 10.4018/IJCWT.2020040103
12. Loi M, Christen M. Ethical frameworks for cybersecurity. In: Christen M, Gordijn B, Loi M. (eds) The ethics of cybersecurity. The International Library of Ethics, Law and Technology, Springer, Cham. 2020. Doi: https://doi.org/10.1007/978-3-030-29053-5_4
13. Dhirani LL, Mukhtiar N, Chowdhry BS, Newe T. Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. Sensors (Basel), 2023; 23(3):1151. doi: 10.3390/s23031151. PMID: 36772190; PMCID: PMC9921682.
14. Maurushat A. Ethical hacking. 1st ed. Canada: Univerity of Ottawa Press. 2019. Doi: 10.1515/9780776627922
15. Hasan M Z, Hussain M Z, Haq H B, Khan R, Nawaz S, Raza Khokhar H, Arshad M. The impacts of ethical hacking and its security mechanisms. Pakistan Journal of Engineering and Technology, 2022; 5: 29-35. Doi: 10.51846/vol5iss4pp29-35
16. Jaquet-Chiffelle DO, Loi M. Ethical and unethical hacking.

In: Christen M, Gordijn B, Loi M. (eds) The ethics of cybersecurity. The International Library of Ethics, Law and Technology, Springer, Cham. 2020. Doi: https://doi.org/10.1007/978-3-030-29053-5_9
17. Coleman E G. *Coding freedom: the ethics and aesthetics of hacking*. 1st ed. Princeton University Press. 2013. https://doi.org/10.2307/j.ctt1r2gbj
18. Pattison J. From defence to offence: The ethics of private cybersecurity. European Journal of International Security, 2020; 5(2):233-254. Doi: https://doi.org/10.1017/eis.2020.6
19. Mancic Z. Cyberpiracy and morality: Some utilitarian and deontological challenges. Filozofija i drustvo, 2010; 21(3): 103-117. Doi: 10.2298/FID1003103M
20. Yaacoub J P A, Noura HN, Salman O, Chehab A. Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. Internet of Things and Cyber-Physical Systems, 2023; 3: 280-308. Doi: https://doi.org/10.1016/j.iotcps.2023.04.002
21. Bhatti M, Zahra A, Mugees Asif M, Ahmad M, Zafar S. Ethical hacking methodologies: a comparative analysis. Mohammad Ali Jinnah University International Conference on Computing (MAJICC). Karachi, Pakistan. 2021. Doi: 10.1109/MAJICC53071.2021.9526243
22. Moneva A, Ruiter S, Meinsma D. Criminal expertise and hacking efficiency. Computers in Human Behavior, 2024; 155: 108180. Doi: https://doi.org/10.1016/j.chb.2024.108180
23. Spafford E H. Are computer hacker break-ins ethical? Journal of Systems and Software, 1992; 17(1): 41-47. Doi: https://doi.org/10.1016/0164-1212(92)90079-Y
24. Hatfield J M. Virtuous human hacking: the ethics of social engineering in penetration-testing. Computers and Security, 2019; 83: 354-366. Doi: https://doi.org/10.1016/0164-1212(92)90079-Y
25. Alashti Z F, Bojnordi A J J, Sani S M S. Toward a carnivalesque analysis of hacking: A qualitative study of Iranian hackers. Asian Journal of Social Science, 2022; 50(2): 147-155. Doi: https://doi.org/10.1016/j.ajss.2022.01.001
26. Wu X, Duan R, Ni J. Unveiling security, privacy and ethical concerns of ChatGPT. Journal of Information and Intelligence, 2024; 2(2): 102-115. Doi: https://doi.org/10.1016/j.jiixd.2023.10.007
27. Rodriguez Duque S, Tal E, Barbic S P. The role of ethical and social values in psychological measurement. Measurement, 2024; 225: 113993. Doi: https://doi.org/10.1016/j.measurement.2023.113993
28. Haywood A. Rewards for hacking -good, bad or ugly? Infosecurty, 2011; 8(1): 42. Doi: https://doi.org/10.1016/S1754-4548(11)70011-0
29. Cohen D, Elalouf A, Zeev R. Collaboration or separation maximizing the partnership between a "*Gray hat*" hacker and an organization in a two-stage cybersecurity game. International Journal of Information Management Data Insights, 2022; 2(1). Doi: https://doi.org/10.1016/j.jjimei.2022.100073