How to Cite:
Kotukh, Y. V., Kislov, D. V., Yarovoi, T. S., Kotsiuba, R. O., & Bondarenko, O. H. (2021). Cybercrime and subculture of cybercriminals. *Linguistics and Culture Review*, *5*(S4), 858-869. https://doi.org/10.21744/lingcure.v5nS4.1769

Cybercrime and Subculture of Cybercriminals

Yevgen V. Kotukh
Sumy State University, Sumy, Ukraine

Denis V. Kislov
Open International University of Human Development Ukraine, Kyiv, Ukraine

Tykhon S. Yarovoi
Interregional Academy of Personnel Management, Kyiv, Ukraine

Ruslana O. Kotsiuba
Legislation Institute of the Verkhovna Rada of Ukraine, Kyiv, Ukraine

Oleksandr H. Bondarenko
National Academy of the National Guard of Ukraine, Kharkiv, Ukraine

***Abstract*---**Unlike traditional types of crime, such as murder or theft, that have a long history, cybercrime is a relatively young phenomenon and a new one that emerged with the advent of the Internet. It should be noted that the very nature of the Internet is quite favourable for committing crimes. Its properties such as globality, cross-border nature, the anonymity of users, wide audience coverage, distribution of main network nodes, and their interchangeability create advantages for cybercriminals who use the Internet at all stages of crime and also allow them to effectively hide from law enforcement agencies. An important aspect of cybercrime that contributes to its spread and hinders the fight against it is the subculture of cybercriminals. This subculture needs to be given special attention, so this issue is discussed in detail in the article. Therefore, the purpose of the article was to analyse cybercrime as one of the youngest types of crime in the modern world. The history of the emergence of cybercrime and cyber-security was considered, the types of cybercrime were characterized, and the functions of cybercrime were analysed.

***Keywords*---**computer, cybercrime, cyber-security, government agencies, hackers.

Corresponding author: *Kotukh, Y. V.; Email: kotukh7080@singapore-uni.com*
Manuscript submitted: 18 July 2021, Manuscript revised: 27 Oct 2021, Accepted for publication: 09 Nov 2021

Introduction

Cybercrime is a crime in a so-called "virtual space". Virtual space (or cyberspace) can be defined as a computer-modeled information space in which there is information about persons, objects, facts, events, phenomena, and processes, presented in mathematical, symbolic, or any other form and in the process of moving through local and global computer networks, or information stored in the memory of any physical or virtual device and other media specially designed for their storage, processing, and transmission (Golubev, 2002). Since cybercrime is inseparable from the information revolution, it should have started in the 1960s. In 1962, Professor John C.R. Licklider published his concept of the widespread Galactic Network (Schweitzer, 2003). This concept assumed that in the future there would be a global network that anyone could connect to and that this network would connect computer systems around the world. In addition to the general idea, Licklider described in detail the fundamental principles of the global network, which later became the basis of the Internet (Hamner, 2009; Halchin, 2004).

The first step towards the emergence of the Internet itself was the creation of the Advanced Research Project Agency (ARPANet) computer communication network, which was commissioned by the US Department of Defence. The idea behind this development was to create a distributed computer system without one clearly defined centre that could be disabled in the event of nuclear war and consisting of interchangeable segments. This is how the principles of the current Internet, such as distribution and globalisation, were already laid down. ARPANet initially consisted of four computers, which were located in major research centres. The network was planned to transmit information and electronic correspondence, so there were no serious access restrictions in its structure, as computer criminals had not yet been foreseen. This quality will be inherited from the Internet in the future, which will lead to its quality of “anarchism”. It is the ill-conceived security and legal control issues in the development of the network's technical principles that will give rise to the problems that the global community will face in the future and that will be one of the main reasons why cybercrime is widespread. The purpose of the article was to analyse cybercrime as one of the youngest types of crime in the modern world (Manky, 2013; De Joode, 2011).

The history of the origin of hacking in the internet and the development of cyber-security

In the 1970s, the first computer criminals appeared, who became known as "hackers". It is hard to say exactly who the first hacker was, but most of the literature on hackers and hackers mentions John Draper as the first professional cybercriminal, who also spawned the first hacker specialisation, phreaker, short for phone hacker. At the time, there were even celebrities such as Steve Wozniak and Steve Jobs, who founded Apple Computers in the future. They established the production of devices for hacking into telephone networks at home. And this is precisely the time that can be considered the beginning of the development of cybercrime. In 1983, the first arrest of an Internet criminal took place in the USA in the state of Milwaukee and became public knowledge. The reason for this was the first registered Internet hack by six teenagers who called themselves the "414 group" (414 – Milwaukee long-distance phone code). Over nine days, they hacked into 60 computers, including those of the Los Alamos State Laboratory. After the arrest, one of the group members testified and the rest were given suspended sentences (Lukatsky, 2010).

Generally speaking, in the eighties there began to be a significant increase in the number of computer attacks. For example, while in 1988 there were only six Internet users' requests for computer attacks to the CERT Internet Security Centre, which opened in 1988, there were 132 requests in 1989 and 252 in 1990. Cybercrime is no longer a rarity; major hacker groups are emerging and the Internet is beginning to be used for a wider range of crimes. This is the beginning of the second phase in the development of cybercrime, featured by the emergence of new specialisations for Internet criminals (Von Solms & Van Niekerk, 2013; Elmaghraby & Losavio, 2014).

In 1984, Fred Cohen published information on the development of the first malicious self-replicating computer programs and applied the term "computer virus" to them. In doing so, he wrote a program that demonstrated the possibility of infecting one computer with another. In 1986, the first computer law, Computer Fraud and Abuse Act was passed in the USA. which prohibited unauthorised access to any computer system and the acquisition of sensitive military information. This law also protected three types of unclassified information: information belonging to financial institutions (e.g., credit card and account information); data belonging to government institutions; and information belonging to international or interstate organisations. Also, the law contained articles prohibiting damage to data (e.g., the spread of viruses). In the same year, Lloyd Blankenship, a member of the Legion of Doom group known as "The Mentor", who wrote the famous "The Hacker Manifesto" Mentor (1986), while serving his sentence in prison, was arrested (see annex). The ideas expressed in this manifesto are still considered the basis of hacker ideology and culture and are widely disseminated on the internet. It is no coincidence that the quantitative surge in cybercrime coincided with the growing popularity of hacker ideas in the computer world, which shows that these phenomena are interrelated (Barber, 2001; Schultz, 2002).

In 1994, the international community learned about the so-called "Vladimir Levin case", classified by the international criminal police as "transnational network computer crimes". An international organized criminal group of 12 people, using the Internet and the Sprint/Telenet data network, having overcome the protection against unauthorized access, attempted to make 40 transfers of money for a total amount of 10 million 700 thousand 952 US dollars from the accounts of clients of the named bank, located in 9 countries, to accounts located in the USA, Finland, Israel, Switzerland, Germany, Russia, and the Netherlands. This was the first major international financial crime using the Internet to become known to the general public and showed that cybercrimes can cause serious financial damage (Beigl et al., 2001; Lindbom et al., 2005).

In 1998, a 12-year-old hacker penetrated the computer system that controlled the drainage of the Theodore Roosevelt Dam in Arizona. The danger of his actions was that if the dam gate was opened, the water could flood the cities of Tempe and

Mesa, with a total population of 1 million people. An assessment of this fact led to the emergence of terms such as “Internet terrorism”, “computer terrorism”, and 'cyberterrorism'. It has also shown that the Internet itself is the most vulnerable to cyberattacks, as its key nodes are accessible from anywhere in the world, which attracts hacker attention (Oli, 2021; Diorditsa et al., 2021).

The emergence of cyberterrorism and the high-profile cases of criminal activity by international gangs show that at this time cybercrime acquired such a characteristic as transnationality. This was the beginning of the third stage in the development of cybercrime. An alarming factor at that time was that the development of the Internet could have had serious consequences not only in the case of intentional cyberattacks but also through the negligence of specialists. For example, in 1997, a Network solutions employee error led to websites whose names ended in ".net" and ".com" becoming unavailable. In other words, the failure of the entire Global Network was due to the inattention of just one person. At the same time, cyberattacks also become a way of achieving political goals. A typical example of this is the internet strike, in which participants of such an action simultaneously visit the site, connect to the service, send e-mails, and write in forums to restrict or even stop access to the site by other users. The website or service is overloaded with external requests, resulting in malfunctions or complete stoppages (Zong & Zhen, 2021; Aryani & Rahayuni, 2016).

The first such action was carried out by a group called the Strano Network, which protested against the French government's policy on nuclear and social programs. On 21 December 1995, this group attacked various websites of government agencies within an hour. At the same time, the group members from all over the world were instructed as follows: they had to use their browsers to access government sites at the same time, which meant that some sites were disabled for a while (Denning, 2001). In the future, the transnational nature of the cybercrime problem is becoming increasingly evident. For example, the conflict in Kosovo is considered to be the first Internet war in which various groups of computer activists used the Internet to condemn the hostilities of both Yugoslavia and NATO, deliberately disrupting the work of government computers and gaining control over sites with subsequent changes in content, the "deface". In parallel, stories about the dangers and horrors of war were spread on the Internet, and various facts and opinions of politicians and public figures were presented, thus making propaganda efforts to a wide audience around the world (Andreev & Davidovich, 2002).

It should be noted that at present almost any military or political conflict is accompanied by an organised confrontation on the Internet. For example, in 2005, there was a wave of cyberattacks triggered by a history school textbook published in Japan that distorted events in China in the 1930s and 1940s, including the silence on war crimes committed by Japanese troops during the intervention. The list of those attacked included Japanese ministries and departments, sites of major Japanese corporations, and sites dedicated to World War II. At the same time, Chinese hackers showed a high level of organisation, as evidenced by the simultaneity and mass scale of their attacks. Knowing the existence of state control over the Internet in China, we can assume that the attack was sanctioned by the state. The use of cyberattacks for political purposes can be considered the beginning of the fourth stage in the development of cybercrime (Mahyudi et al., 2017; Widana et al., 2020).

China was followed by Russian hackers who carried out several large-scale DDoS attacks (distributed denial-of-service attacks). In late April and early May 2007, for example, Estonian government websites were attacked for several days. The "Nashi" youth movement took responsibility for this. And in August 2009, the American edition of Aviation Week accused Russian hackers of attacking the Baku-Tbilisi-Ceyhan pipeline server. According to the publication, the attacks were carried out from the same addresses as the attacks on Estonian websites (Lemos, 2011). Thus, four stages in the development of cybercrime can be identified so far:

- Stage 1. The emergence of cybercrime and the hacker subculture.
- Stage 2. The spread of cybercrime, the emergence of specialisation of cybercriminals, and national hacker groups.
- Stage 3. The transnational nature of cybercrime, the emergence of cyberterrorism, and international hacker groups in all areas of cybercrime.
- Stage 4. Use of the Internet for political purposes, the emergence of such phenomena as Internet strikes and Internet warfare, targeted use of cyberattacks against governments of individual states.

The concept of the subculture of cybercriminals in the modern world

By analysing the nature of cybercrime, the following characteristic features can be highlighted:

- The intellectual nature of cybercrime – committing a cybercrime requires a certain amount of knowledge, and intelligence among cybercriminals is promoted by the subculture of hackers, which gives them an incentive for intellectual self-development.
- Cybercrime, unlike other intellectual crimes, is accessible to people of low social and age opportunities - to commit cybercrime one does not need to have a high social position, it is enough to have access to the internet and a computer.
- Anonymity and non-personation of cybercrime - mechanisms for identifying in the global network allow an individual to carry out transactions anonymously or impersonate another person, change their biographical information or social status.
- The remoteness of cybercrime – the perpetrator and the victim may be thousands of kilometers apart, as there is no difference in committing a crime against computer systems located on a neighboring street or in another country if the crime is committed via the internet (Kurakov & Smirnov, 1998).
- High latency of cybercrime, one of the main reasons for which is that damage from cybercrime often seems insignificant to the victim in comparison to an investigation procedure that can take time but does not guarantee prosecution of the perpetrator or compensation for damages (Kesareyeva, 2002).

- Transnationality of cybercrime - according to some authors, about 62% of computer crimes are committed as part of organised groups, including those in several countries (Dolgova, 2003).
- The rapid growth of cybercrime, which is due to the increasing spread of the internet in various areas and the cheapening of internet services.

It is clear that cybercrime is not standing still, new types of crimes committed through cyberspace are emerging and will continue to emerge. However, to date, among the most typical types of cybercrime that pose a threat to national security, are the following:

- Crimes against constitutional human and civil rights and freedoms, such as violation of privacy, violation of the confidentiality of correspondence, telephone conversations, postal, telegraphic and other communications, violation of copyright and related rights.
- Crimes against life and health. The first recorded case of murder committed via the Internet was in February 1998 in the USA. A seriously injured witness to the crime was hidden in a closed hospital on the grounds of a military base, but criminals changed the operating modes of the pacemaker and lung ventilator via the Internet, which led to the death of the witness. Also, sites promoting drug addiction, publishing the technology of manufacturing narcotic drugs on a domestic or industrial scale; distributing narcotic drugs, psychotropic substances, and their analogues have acquired alarming proportions on the Internet.
- Crimes against honour and dignity. Anonymity and a wide audience of the Internet provide unlimited opportunities to disseminate information of any kind, including slanderous, defamatory, defamatory of honour and dignity.
- Crimes against property. Internet fraud is one of the most common types of crime on the Internet today, and new forms, types, and methods of fraud are appearing every day.
- Crimes in the area of computer information, primarily such as unauthorised access to information and the creation, use, and distribution of malicious programs.
- Crimes against public morality. For example, the porn business has become widespread on the Global Network, with porn sites on the Internet accessible to any part of the world and any category of the population, and distributors of immoral products feel impunity because they act anonymously.
- Crimes against state security. With the increasing use of the Internet in state structures, it is possible to gain illegal access not only to private and corporate information, but also to information that is a state secret, and to commit crimes such as espionage, treason, or disclosure of state secrets via the Internet.

The Internet is now not only a fundamentally new means of mass communication, it covers almost all areas of human activity. Many processes are successfully transferred from the physical world to the virtual world, while the global Internet itself creates conditions for the formation of virtual communities, generates linguistic forms of a new type, erases the borders between states, ignores the distances that separate people, and, ultimately, generates specific forms of culture. It can be argued, however, that the criminal subculture on the Internet is ideologically and externally very similar to and part of the hacker subculture. It is known that the hacker subculture was originally asocial, opposing the state and society. Therefore, for today's cybercriminal, the hacker ideal is not only a way of making a profit but also of justifying his crimes and gaining recognition and respect in virtual space.

Some researchers have identified the Internet user community as a kind of subculture, one of the foundations of which is information liberalism (Smirnova, 2000). In this case, hackers can be called the "radical direction" of this subculture, as they are prepared to commit several crimes for the sake of freedom of access to information. One can agree with Denisov (2002), who believes that a subculture is a set of norms and rules of behaviour, traditions, customs, and external paraphernalia that exist within a certain social micro group of people united by some common interest (professional or otherwise); supported by all members of this group and different from those generally accepted in society. It is usually defined as a system of shared beliefs, relationships, and symbols that differentiate a particular micro-group within a large cultural community.

Based on this definition, the hacker subculture can now be considered an established one. They have a specific lifestyle; specific norms, values, preferred behaviour patterns, and external distinguishing attributes that are characteristic of a given social group. At the same time, the hackers' ideological base is based on liberalised access to information. "We investigate, and you call us criminals. We are in search of knowledge and you call us criminals" is an excerpt from the famous manifesto of hackers (The Hacker Manifesto), written by a hacker under the pseudonym (Mentor, 1986). This thesis is supported by most of the online community. For example, even in China, where the tradition of liberalism is not as widespread as in other countries, there is a tendency for "netizens" to fight for free coverage of important events via the Internet (Qiang, 2003).

The authors are not unjustified in their support for freedom of information, and their slogans are often supported by serious and well-thought-out arguments that are philosophically, culturally, and logically sound. For example, Kaspersky (2005), writes: “The situation has reached logical absurdity, and riots have smelled in the air. A revolt against the totalitarianism of the democratic regime, when one nosy businessman takes away from humanity what is rightfully his. Information is a publicly available resource, just like water and air. We are the children of our culture. Our thoughts and judgments, which we sincerely consider to be our own, are a combination of what has long been invented and expressed. Successful discoveries and bright ideas are all the result of reflection or rethinking. Once heard or read”.

For the hacker, the right to freedom of information is more obvious and logical than patents, copyrights, or state secrets. That is, within a hacker's subculture, the right to information simply does not work because, "to operate within a particular culture, the right must be recognised and justified as such" Danilyan (2006), and that "the right must be compatible with human moral values" (Nersesyants, 2004). Their rejection of consumer culture can also be highlighted.

This is evidenced by the "cracking notes" written by a hacker under the pseudonym "Orc+", which is imbued with a hatred of the existing social system. Also, important aspects of hacker ideology are the belief in the computer's ability to change lives for the better and the rejection of any authority outside the virtual space and the denial of racial, religious, and social differences. The hackers' subculture differs significantly from other criminal cultures, but at the same time, some similarities can be found. For example, Tulegenov (2003), distinguishes several differences between criminal subcultures. They are characterized by rapid variability, as the criminal world has always been highly adaptable and able to adapt to changing conditions. This also applies to hacker culture. In other words, perhaps the hacker subculture differs significantly from the "typical" criminal subculture.

First, Tulegenov (2003), states that criminal subcultures do not leave a material legacy, i.e., they do not have any material carriers other than the criminals themselves, and are passed on from mouth to mouth. This is not the case with hackers. Secondly, the criminal subculture is a closed system and has its own hidden, most often dangerous, attitudes that are contrary to society. The hacker subculture is also a closed system, but hacker values have a well-defined philosophical basis, and this gives hacker ideas some legitimacy. Thirdly, almost all criminal subcultures use pseudonyms. In hacking environments, they are called "nicknames" (nick, nickname). However, pseudonyms are accepted not only in the criminal Internet subculture, but also in the entire Internet community, and unlike pseudonyms in the criminal environment - "nicknames", everyone chooses for themselves. As in other criminal subcultures, nicknames may reflect character and behaviour patterns; transformed surnames and names; status in a group; appearance or social status patterns; preferences in music, literature, art; the specifics of criminal activity and the place of commission. However, there are no nicknames in a hacker's environment that are similar to a prison or common criminal nicknames, as well as humiliating or ridiculing defects. Fourthly, as in all subcultures, the criminal subculture of hackers has its jargon. However, unlike general criminal jargon, which is a derivative of the national language, modern hackers' language, regardless of their country of residence, is full of English words, and often the hacker's language is inaccessible to ordinary users, although many words are also used in the non-criminal environment of computer professionals. Fifth, if we talk about other external attributes of hacker culture, it should be mentioned that, unlike other criminal subcultures, hackers have their periodicals, fiction, films, videos, and posters. Other categories of criminals are satisfied only with specialised internet sites; for example, there are internet portals that focus on the drug offender. And the importance of literature and films for hackers should not be underestimated. Of course, for professional hackers, most stories may seem ridiculous and far from reality, but for the majority of the population (especially teenagers) hacker works of art form an ideal to aspire to, instil hacker values in an easy and accessible form, demonstrate patterns of behaviour, and the hacker image itself is highly romanticised and therefore attractive.

The above shows that although the general criminal subculture and hacker culture are somewhat similar, they are still quite far apart. Some ideologists of the hacker movement also agree with this fact. For example, Kaspersky (2004), the author of the books "Techniques and Philosophy of Hacker Attacks", "Techniques for Debugging Programs without Source Code", etc., describes a hacker as follows: "There is an opinion that there are some signs of belonging to hackers. These are long (unbrushed) hair, beer, cigarettes, pizza in unlimited quantities, and a wandering look in space such signs are not the cause but the consequence. Being attached to a computer makes it more economical to treat your free time, sometimes eating snippets and on the move. Long hair? Yes, it is characteristic of all computer people (and not just them), not just hackers, like, by the way, all other hacker signs". However, this and other similar opinions cannot overshadow the fact that today's hacker subculture still has a criminal basis, since it can be defined as a set of ideas, values, customs, traditions, and norms of behaviour aimed at organising a way of life that aims to commit, conceal and evade computer crimes. At the same time, the value complex of this subculture serves to legitimise and promote the idea of hacking in society, which is why a person who shares the values of a hacker is ready for an Internet crime or approves of crimes committed by others.

It should be noted that the subculture of hackers would not have been so important to the development of cybercrime if it had not performed several important functions. At present, there are several criminological and sociological studies Denisov (2002); Pavlova (2004); Tulegenov (2003); Rassolov (2003), that highlight the functions of negative and criminal subcultures. The most important of these for cybercrime are the following:

- Unifying. The fact that hackers all over the world have similar ideologies, views on life, ways of earning a living, and use the same literature, terms, and slang is a major unifying factor that makes it easy for hackers to join international groups to commit socially dangerous acts, share professional information and criminal instruments.
- Legitimisation. Justification in the eyes of others and compliance with their moral and ethical beliefs about crimes on the Internet provides an additional incentive for choosing a criminal path when achieving a goal. The lack of explicit public condemnation of such illegal behaviour leads to a situation where cybercriminals not only do not hide but also show off their illegal achievements without fear of responsibility, leaving brand names or slogans of hacker groups at crime scenes (which they ironically often call “copyright” (Kaspersky, 2004)). Also, as mentioned above, hackers themselves do not consider their activities to be criminal, which gives them a romantic image.
- Information. It is within the subculture that ideological and instrumental information is disseminated. In a hacker environment, new ways and modern means of committing cybercrimes are transmitted. Through their subculture, hackers learn how to get away from law enforcement and how to destroy evidence, which methods of extracting money by criminal means are safest and which means are most effective. Thanks to the information disseminated in the hacker environment, cybercriminals often have a technical advantage over private security services and government counter-crime services.
- Criminogenic. This function is expressed in the accumulation, preservation, and transmission of traditions of the criminal Internet environment, which

is capable of opposing social institutions, i.e., ensuring the reproduction and spread of cybercrime.

Conclusions

Thus, as can be seen, the hacking subculture is one of the main criminogenic factors of cybercrime, so neutralising the negative effects of this subculture is the most important way to combat cybercrime in general and the first and third types of cybercrime in particular. This area should include ideological and promotional prevention measures aimed, on the one hand, at eliminating anti-social attitudes in certain groups and individuals (computer specialists, technical students, etc.). At the same time, propaganda should not be limited to the statement that it is not permitted and prohibited by law to do so but should have a serious philosophical and ideological basis opposing the hacker subculture.

On the other hand, measures aimed at the general public should be taken to develop a negative public attitude towards cybercriminals and their actions. Unfortunately, a certain idealisation in the public consciousness of the unlawful activities of hackers hinders the fight against cybercrime and creates additional incentives for criminal acts in cyberspace. It is, therefore, necessary to introduce into the public consciousness the idea that hackers are not modern Robin Hoods or "freedom fighters" but criminals, and it is necessary to widely publicise the negative consequences of their activities for individuals, society, and the state. This can be helped by social advertising tools presented in various media as part of large-scale campaigns such as "No to cybercrime!" or "Are you a hacker? You are a loser!". Taken together, this would allow the formation and development of certain groups of people, especially adolescents and young people who are prone to criminal behaviour, to be controlled over time and would lead to a reduction in anti-social attitudes, attitudes, and values among them, which would ultimately reduce the basis for cybercrime.

References

Andreev, A., Davidovich, S. (2002). On information confrontation during the armed conflict in Kosovo.

Aryani, I. G. A. I., & Rahayuni, N. K. S. (2016). Innovation of teaching and learning english applied to animal sciences' student with the combination of computer media and audio visual. *International Journal of Linguistics, Literature and Culture*, *2*(1), 1-7. Retrieved from https://sloap.org/journals/index.php/ijllc/article/view/78

Barber, R. (2001). Hackers profiled—who are they and what are their motivations?. *Computer Fraud & Security*, *2001*(2), 14-17. https://doi.org/10.1016/S1361-3723(01)02017-6

Beigl, M., Gellersen, H. W., & Schmidt, A. (2001). Mediacups: experience with design and use of computer-augmented everyday artefacts. *Computer Networks*, *35*(4), 401-409. https://doi.org/10.1016/S1389-1286(00)00180-8

Danilyan, O.G. (2006). Philosophy of law. Moscow: Publishing House "Eksmo".

De Joode, A. (2011). Effective corporate security and cybercrime. *Network Security*, *2011*(9), 16-18. https://doi.org/10.1016/S1353-4858(11)70097-6

Denisov, N. L. (2002). Influence of criminal subculture on the formation of the personality of a minor criminal: Dis.... cand. jurid. sciences.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. *Networks and netwars: The future of terror, crime, and militancy*, *239*, 288.

Diorditsa, I. V., Telestakova, A. A., Koval, O. M., Nazarenko, O. A., & Nastiuk, A. A. (2021). Information interventions as a new dimension of Ukraine's cyber-vulnerability. *Linguistics and Culture Review*, *5*(S2), 152-166. https://doi.org/10.21744/lingcure.v5nS2.1337

Dolgova, A. I. (2003). Crime, its organization and criminal society. *Russian Criminology Associations, Moscow*, 191-194.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research*, *5*(4), 491-497. https://doi.org/10.1016/j.jare.2014.02.006

Golubev, V.A. (2002). "Cyber terrorism" – myth or reality?

Halchin, L. E. (2004). Electronic government: Government capability and terrorist resource. *Government Information Quarterly*, *21*(4), 406-419. https://doi.org/10.1016/j.giq.2004.08.002

Hamner, M. (2009). Expanding the technology acceptance model to examine personal computing technology utilization in government agencies in developing countries. *Government information quarterly*, *26*(1), 128-136. https://doi.org/10.1016/j.giq.2007.12.003

Kaspersky, K. (2004). Technique and philosophy of hacker attacks. Moscow: SOLON-Press.

Kaspersky, K. (2005). *Shellcoder's Programming Uncovered (Uncovered series)*. БХВ-Петербург.

Kesareyeva, T. P. (2002). Criminological characteristics and crime prevention in the Russian segment of the Internet: abstract of dissertation for the degree of candidate of Law. Moscow: University of the Prosecutor's Office of the Russian Federation.

Kurakov, L. P., & Smirnov, S. N. (1998). Information as an object of legal protection. *Helios*, 18.

Lemos, R. (2011). Cyberterrorism: The real risk.

Lindbom, L., Pihlgren, P., & Jonsson, N. (2005). PsN-Toolkit—a collection of computer intensive statistical methods for non-linear mixed effect modeling using NONMEM. *Computer methods and programs in biomedicine*, *79*(3), 241-257. https://doi.org/10.1016/j.cmpb.2005.04.005

Lukatsky, A. (2010). Hackers control reactor.

Mahyudi, J., Saryono, D., Siswanto, W., & Pratiwi, Y. (2017). Construction of visual features of Indonesian digital poetry. *International Journal of Linguistics, Literature and Culture*, *3*(5), 1-13. Retrieved from https://sloap.org/journals/index.php/ijllc/article/view/218

Manky, D. (2013). Cybercrime as a service: a very modern business. *Computer Fraud & Security*, *2013*(6), 9-13. https://doi.org/10.1016/S1361-3723(13)70053-8

Mentor. (1986). The hacker manifesto.

Nersesyants, V. S. (2004). Problems of the general theory of law.

Oli, M. C. (2021). Proficiency amidst COVID-19 challenges in developing computer programs: An outcomes-based approach in discrete structures. *Linguistics and*

Culture Review, *5*(S3), 770-783. https://doi.org/10.21744/lingcure.v5nS3.1593

Pavlova, A. A. (2004). Subculture of shadow economic activity: Essence and factors of reproduction in Russia: abstract of dissertation for the degree of candidate of Sociology. Moscow: Russian Academy of Public Administration.

Qiang, X. (2003). China's Virtual Revolution. *Project Syndicate*.

Rassolov, I. M. (2003). Law and the Internet. Theoretical problems. Moscow: Publishing House “NORMA”.

Schultz, E. E. (2002). Taking a stand on hackers. *Computers & Security*, *21*(5), 382-384. https://doi.org/10.1016/S0167-4048(02)00501-1

Schweitzer, D. (2003). *Incident response: computer forensics toolkit*. Wiley.

Smirnova, I.A. (2000). The virtual space of culture. In Materials of the scientific conference on April 11-13, 2000, (pp. 148-149). St. Petersburg: St. Petersburg Philosophical Society.

Tulegenov, V. V. (2003). Criminal Subculture and Its Criminological Meaning/Tulegenov Vadim V.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Widana, I.K., Dewi, G.A.O.C., Suryasa, W. (2020). Ergonomics approach to improve student concentration on learning process of professional ethics. Journal of Advanced Research in Dynamical and Control Systems, 12(7), 429-445.

Zong, F., & Zhen, S. X. (2021). The link between language and thought. *Macrolinguistics and Microlinguistics*, *2*(1), 12–27. Retrieved from https://mami.nyc/index.php/journal/article/view/12