Videogames in Cybersecurity: Philosophical and Psychological Review of Possible Impact

Levyk Bogdan †, Mariia Maletska ††, Svitlana Khrypko ††, Kryvyzyuk Leonid †††, Dobrodum Olga ††††, Katerina Pasko †††††

levukbs@ukr.net momaletska.iff19@kubg.edu.ua s.khrypko@kubg.edu.ua

†Regional Scientific and Educational Center "Holodomor, Holocaust, International Dialogue" Lviv Polytechnic National University, Lviv, Ukraine

††Department of Philosophy, Faculty of History and Philosophy, Borys Grinchenko Kyiv University, Kyiv, Ukraine

†††Department of Military Intelligence, Analysis and Prognosis of Socio-Political Processes, Hetman Petro Sahaidachnyi National Army Academy, Kyiv, Ukraine

††††Department of Culturology and Philosophical Anthropology of the National Pedagogical Dragomanov

†††††Department of Psychology Educational-Scientific Institute of Pedagogy and Psychology of Sumy State Pedagogical University named after A.S. Makarenko

Summary
An issue of security and threat is urgent as well as it concerns everyone: a person, community, state, etc. Today, the question of cybersecurity has become especially relevant due to general digitalization and the spread of the cyberculture. In terms of it, the growing popularity of videogames can be observed. Their impact on society differs significantly, therefore, it needs thorough consideration. The purpose of the article is to disclose the role of videogames in cybersecurity. To achieve the stated purpose, such methods as analysis, synthesis, systematization and practical involvement of videogames have been used. As a result, three levels of possible threat of videogames has been distinguished: videogames as a possibly dangerous software, as a tool of propaganda and spread of stereotypes, as a space for the creation of virtual communities. In conclusion, it is stated that videogames can be not only a threat, but also a tool for strengthening the cybersecurity.

Key words: ***Security, cybersecurity, videogame, digital psychology, videogame philosophy.***

1. Introduction

An issue of security and threat is urgent as well as it concerns everyone: a person, community, state, etc. A fact of security provides the ground for life, personal purpose realization, needs, wishes. A threat strengthens the urgency of security, provides a stimulus for looking for new tools to ensure it. Security is a core of different contexts' consideration and realization, namely national security, state security, information security, territorial or ecological security, etc. The necessity of security is considered as "a human need in stability, protection from anything that can cause harm" [1] in the context of hierarchy of human needs. The specific case of today's security is cybersecurity. In digitalized society, where many important processes are transferred to cyberspace, the consideration of possible virtual threats is especially relevant. There are new phenomena in contemporary digital culture, which may constitute a threat to the state's cybersecurity. One of these phenomena, that is steel underexplored despite the scientists' wide interest is the videogame phenomenon.

Today, the growing popularity of videogames can be observed. They are used for learning [2], act as a space of communication, which has been especially relevant during the COVID-19 pandemics [3]. The impact of videogames differs significantly from the other media due to their high interactivity. Therefore, it needs detailed consideration with proper attention payed to its specifics.

In case of security, videogames can pose unpredicted threats on various levels of human existence. However, these threats are usually considered separately, without general comprehension of videogames as a phenomenon which has possible negative impact namely on the area of security. On the other hand, the researches that consider videogames as a threat, usually do not pay attention to their possible use to strengthen the security. Therefore, *the purpose of our article* is to disclose the role of videogames in cybersecurity.

2. Methodology

With the help of analysis, synthesis and grounded theory study, security concepts have been analyzed and the cybersecurity phenomenon has been considered, the specifics of cyberspace has been revealed. To study videogames and peculiarities of their use, both analysis of existing works and practical involvement in the game process have been used due to the fact that such phenomena as videogames can only be studied in combining theory with practice. According to E. Aarseth [4], we can study videogames in three ways: firstly, considering the design, rules and mechanics; secondly, reading reviews and reports;

Manuscript received July 5, 2021
Manuscript revised July 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.7.29

thirdly, playing by ourselves. All ways of study are valid, however, the third is considered the best method, especially in combination with other two ways, due to the fact that without personal experience, severe misunderstandings can be committed, even after studying the mechanics and information about the games. Looking at this phenomenon both from "inside" and "outside", we can stay unbiased and analyze videogame from different positions. Theoretical studying videogames is possible only when we talk about technical part of games. When it comes to the context, the absence of direct work with the game process or, at least, with the so called "let's plays" and professional reviews of games can narrow the results to one point of view without consideration of other dimensions of the analyzed phenomenon.

After the thorough study of practical impact of videogames on the cybersecurity, its possible usefulness has also been considered with the help of systematization as philosophical method.

3. Results and Discussion

3.1 Cybersecurity and cyberspace concepts

Cybersecurity can be considered from different perspectives: as methods to detect potential intruders and the ability to protect the cyberspace from cyber-attacks; safeguarding of computer networks and the information in them from penetration, damage and disruption; means of reducing risk of malicious attack to software, computers and networks; collection of tools, policies, concepts, guidelines etc. that can be used to protect cyber environment and organization. The main terms of definitions, therefore, are "to protect", "property rights", "capabilities" and "assets" [5]. Different nations also define their cybersecurity strategies differently: as means related to the confidentiality, availability and integrity of information processed, stored and spread through electronic and similar means; as an appropriate level of response to cyber-attacks; as an information system that can resist properly to threats in ICT systems; a practice of making the network as secure as possible etc. [6]. From the considered definitions, we can see that the central concept of cybersecurity is the "security". The history of "security" definitions is characterized by the multi-dimensional context of its usage and relevance of the issue simultaneously. A fact of security, guarantees of security, search of security implementation are urgent for everyone in any period of state development – from the ancient times till postmodern information society, in which we live today.

Aristotle presented the security as the main criteria of ideal society [7]. According to B. Spinoza, "peace and security" is a main aim of civil society establishment [8]. J.-J. Rousseau claimed that the main care of a state should be "care for self-preservation" [9]. Thomas Hobbes highlighted the importance of security factor, namely, he mentioned that a war of all against all happened under the natural life circumstances. Human fear for personal security is a consequence of the war. A man is forced to seek the means of collective security against the mentioned threats; as a result, a state is created to which a human transfers a part of natural human rights. Locke claimed that each human had a right to manage and protect his personal life, freedom, property and so on. Nevertheless, the rights were not always secured under the natural conditions as not all people respected the rights of others. People created a state to secure themselves by signing a social agreement. A state, as an embodiment of social agreement, was not created only for rejection of personal rights in favor of it, but for the higher level of insurance of personal rights that was impossible under the natural conditions [7]. A list of statements and considerations of the famous thinkers can be continued, and it only proves a fact of urgency of security issue. A state was considered to be a fundamental base for social security guarantees in general and a singular citizen in particular. However, today, in view of globalization and digitalization, the state is not always able to protect a singular citizen and a community as a whole in a cyberspace. Being different from the physical space, cyberspace unfolds on two levels: it has its physical part (a network of computers or other technical means which constitute the basis for virtual interaction) and the virtual part (the virtual environment which people enter with the use of the physical part, i.e. hardware with the specific software). Cyberspace changes the perception of time and distance, it lives according to its own temporal and spatial specifics [10]. Due to the change in spatial dimension, many things work differently in cyberspace. For example, spying in cyberspace differs significantly. It does not necessarily need intruding on foreign territory – cyberspy can stay on their home territory and act through the cyberterritory on another sovereign country [11].

Considering this, we can state that, while in physical space, security can be provided by the means of defending the territory, cybersecurity lies not in the boundaries of the territory as some spatial parameter, but in virtual area where information is generated and transferred. Each phenomenon that creates a part of cyberspace or functions in it has can be a potential threat; however, videogames can pose this threat on several levels due to their specific structure.

3.2 Videogames as a specific phenomenon in cyberspace

Videogames are usually defined as a way of interaction between a player, a machine with an electronic visual display, and possibly with other players, mediated by a meaningful fictional context, and which is supported by an emotional connection between the player and the results of his action in this fictional context. Features that researchers usually consider characteristic of videogames are,

therefore: interactivity (interaction) with the player; a formal system based on rules as a core of a videogame; fictional context: the need for technical support [12, 13, 14, 15, 16, 17]. Although the term "videogame" is based on the word "game", most researchers do not define videogames as games. Videogames, similarly to games, are based on rules, however, their purposes are different. Violation of the rules underlying the game leads to a violation of the game itself and the exclusion of the player who violates the game from the gaming community. Within videogames, in addition to the rules that define the actions and goals of the game, there are so-called meta-rules that determine the possibility of changing and modifying the videogame [18]. Violation of videogame rules is impossible without changing the software logic of a videogame, or so-called cheating [19]. Videogames are a specific case of software, therefore, for understanding their impact on cyber security, both content and technical levels should be properly considered.

Talking about the content, we should say that another important feature of videogames, which distinguishes them from other cultural products, such as literature, cinema, etc., is interactivity. It is the possibility of interaction that allows immersion of the player into the game, strengthens the persuasiveness of what is happening in the game world. In addition, due to interactivity, the game can evoke more emotions in the player, which, in turn, helps to consolidate impressions, ideas, identify features and characteristics with certain images. Such impact is much higher than impact of other media, because in most videogames, player directly participates in in-game events, and can form view on real events according to their presentation in videogames.

In addition to the consideration of videogames on the levels of the software base and the content, attention should be payed to the level of interpersonal communication which is possible in some videogame genres. On the basis of game rules and specific content, fictional context, the interaction between player in the videogame world with the use of gestures, in-game emails and chats etc. occurs, therefore, creating another level of perceiving the videogame phenomenon.

3.3 The possible threat of videogames

Considering the specific structure of videogames, mentioned above, we have distinguished the following levels of possible threat of videogames to the national cybersecurity:

1. Threat of videogames as a specific case of the software (the software level of videogame phenomenon);
2. Threat of information given through videogames (propaganda through videogames, the level of videogame content);
3. Threat of videogame communities (the level of interpersonal interaction in videogames of particular genres).

Talking about videogames as a software, we should mention the fact that in many multiplayer games, there are weak points in the game system, through which cyberattacks can be performed and players' data can be stolen. Fraud in videogames is usually based on misusing of the game environment, however, while in-game cheating (violation of the game rules) is a problem of the videogame space and usually it cannot be harmful for person's or state's security, fraud in videogames involves violation of national and international law, and may also extend to external media, such as Web forums and email [20]. Vulnerability of videogames as specific type of software, therefore, is the first possible threat to cybersecurity. It can be used to receive information about another state' citizens, their preferences, finances etc.

Considering the content of videogames, they can pose a threat through transferring misinformation, misrepresenting other states and their policies. Videogames can act as means of propaganda, which becomes more effective because of their interactivity. With the immersion into game environment, player perceives information and actions differently than simply watching events on TV or reading about them. In games, a player is a part of these events [21]. Videogames use various propaganda techniques, such as name calling and labeling (in dialogues, narratives, in-game books, newspapers etc.), referencing and appeal to authority, martyr technique, demonization of the enemy, double-speak and many others [22]. All mentioned techniques transfer and strengthen stereotypes existing in society.

The constant creation of stereotypes is an integral characteristic of social processes, the features of which are determined not only by the nature of these processes, but also by the specifics of the objects of stereotyping. Objects of social stereotyping are not always available to the perception of the individual: the perception of these objects is not direct and is not usually performed through empirical experience, it is indirect – mainly through information broadcast by the media.

The theoretical basis of the theory of stereotypes was W. Lippmann's postulate of incomprehensibility for the individual of the world of politics, the impossibility of verifying political reality based on individual consciousness. In "Public Opinion", the researcher pays great attention to the manipulative role of the media, absolutizing, according to many scholars, their role in the process of stereotyping. Stereotypes are defined as generalized, stable, emotionally charged, socially valued ideas about social objects that are assimilated by the individual in the process of social interactions, poorly reflected and can be automatically reproduced sometimes throughout life. Stereotypes are also considered common notions of attributive personality traits. The prevalence of stereotypical representation does not

allow to consider it a reflection of the true properties of the object [23]. The political stereotype, respectively, is the individual's perception of political objects that are assimilated in the process of social interactions and the assimilation of information that in some way relates to the political sphere. Stereotypes spread by the media influence the further society's attitude towards war and peace, other nations' actions, political leaders and their words.

In videogames, we can find stereotypes that concern nations (for example, here we can mention "Command & Conquer: Red Alert" series), political leaders, marking them "good" or "bad" not on the basis of real events, but on the basis of events happening in in-game reality. The decisions made by political leaders in real life after playing games with deep immersion can be perceived through their image in games. Therefore, the image of the enemy can be formed through videogame content and the aggressive actions can be disregarded because of their misrepresentation in videogame content.

One of the brightest stereotypes transferred through videogames is the image of totalitarian states and totalitarian leaders. In these videogames, not only existing political figures are demonstrated, but also the general concept is created with the particular features inherent in real totalitarian states. Here, we should mention such videogames as "Beholder" and "Papers, Please" as the brightest example of the spread of stereotypes in videogame content.

"Beholder" is a story videogame, the events of which unfold in the unnamed country, which is under the leadership of the "Great Leader". The protagonist of the first part, Karl, replaces the man who was recently arrested. In an atmosphere of constant lack of resources, Karl has to monitor the residents of the house and write denunciations against them. The videogame is made in black and white, which depresses the player and enhances the effect of choosing between morality and survival. In the monuments to the "Great Leader" shown in the game, the features of totalitarian dictators, quite simplified and recognizable to the average player, can be seen. In "Beholder" the player faces a deficit, oppression of the authorities, constant directives of the authorities that prohibit certain things. For example, the game directive №6053 prohibits reading books. Newspaper articles and conversations of the characters also reflect the main stereotypes of totalitarian rhetoric.

"Papers, please" is a videogame in which the player has to check the documents of people crossing the border and decide their fate. This videogame was considered by researchers primarily from the moral and ethical point of view, because it raises a set of moral themes, such as dehumanization, privacy, honesty through a simple game mechanics built on the document verification [24]. The environment in which the events of the game take place reflects a set of stereotypes by which the prevailing regime and ideology in the state can easily be recognized. This is not directly stated in the game, but this impression is formed by the constant strengthening of rules and oppression, supervision of citizens by the state. The protagonist and people crossing the border are constantly forced to fill out additional certificates, the number of which is growing almost every game day. Under certain conditions, the protagonist's curator can report him, after which he is sent to hard labor, and the story about this, like most information letters in the game, ends with the words "Glory to Arstotska!". You can leave the country where the game takes place by forging a passport and a pass. All this is complemented by appropriate musical accompaniment and appropriate graphics in pastel and gray shades. Thus, the player is immersed in an atmosphere of depression, constant pressure and deteriorating conditions, intimidation, where he has to choose between himself and others, often in his favor.

Stereotypes that show political regimes are not the only vividly demonstrated ones in videogames. Military shooters also change the perception of war and peace, therefore, they also change one's own attitude to the homeland and foreign states. Military videogames connect different past, present and future events on the background of the real military actions, they engage player into the violence and prevent him from it at the same time [25]. Being a phenomenon of popular culture, videogames can support military actions and/or conflicts. Videogames also may describe past military events distorted, lead to the shift of representation of historical events and it can be said that videogames engage player into the military activity indirectly through the engagement in videogame environment [26], which, in turn, can change the attitude to real war, which strengthens the role of videogames as a propaganda tools. We do not consider videogames as phenomenon that causes violent behavior, however, it should be noted that, as other media, videogames may be used to legalize violence and to mark people engaged into warfare as "good" or "bad" according to the tasks of author of the content shown in the videogame. While on the first two levels of the possible threat of videogames, the state can use some measures to defend its citizens, the third level is the most difficult to regulate. It is the level of interpersonal communication and creation of virtual communities within the videogame space.

Such a phenomenon as virtual communities deserves special attention in the field of information culture and cyber security.

Depending on the context and purposes of creation, for a person, virtual reality can act in its various forms:

- to be an information and communication environment and artistic and aesthetic space; to create a game situation and at the same time include fragments of real life, increasing the complexity of understanding and evaluating what is happening;

- to form a special psychological state that reveals a person's world of new emotions and feelings, blurs the distinction between real and unreal; to be a special educational environment;
- to act as a quasi-society - a special type of "unrealistically existing" socio-cultural space, a kind of existential mode of "virtual human" [27].

The virtual community as an innovative subculture consequently represents quite specific and mostly negative contexts of one or another activity. For example, this leads to the formation of a new generation of people who identify with other people simultaneously "coexisting" in two spaces – social and virtual, but prefer to work and relax, communicate and have fun in the network space. Additionally, these people cannot be attributed to suppressed minorities or groups ignored by society. Virtual culture is gradually forming a special type of person, the formation and development of which is largely determined by the system of network interactions. Anonymous sociality, mixed or contrived identity, neutralized anthroponymy (names, surnames, patronymics), propensity for spontaneous flashmobbing, covert control, extraterrestrialism and extra-institutionality – these are just a few of the factors that work for no good of national security established concept. Understanding the problems of virtual communities, researchers often turn to the idea of a "third space", which is understood as a place separate from home and work, i.e. it is certain public places in the territorial collectivity, such as cafes, clubs, bars and the like. As "third places" lost their significance during suburbanization, the traditional communities associated with them disintegrated. But the need for communities remained, and it was able to be implemented through the development of computer networks and the emergence of virtual communities in which forms and methods of social exclusion, such as gender, religion, race or class, lose their significance [28].

Virtual communities are a place where the individual is free from the social barriers that arise from the physical embodiment of identity. In virtual reality, a person experiences specific solitude [29], which makes him a part of a community without physical inclusion. Virtual communities with the whole set of postmodern factors and constants are, without a doubt, an attractive phenomenon. In them, one can hide his real name, which is important part of social existence and perceiving personality by others [30] It is no coincidence that some virtual communities already number millions of people, but a certain danger lies in it. Today, virtual time for many people becomes a time of anonymous sociality, because they have a combination of social and virtual time. Therefore, society and the state must be aware of the full range of dangers and risks of long-term human stay in quasi-society, take responsibility for cultural forms and practices, patterns of behavior replicated in information and communication systems, given that qualitative characteristics of artificial environments "set" the sociocultural program of modern human. That is why the issue of communicative culture ecology as such becomes especially relevant. The passion for cultural innovations (such as virtual communities) should not undermine the established traditional norms and rules of cultural communication. After all, it is the communicative component that unites the past, the present and the future.

Due to the powerful polycontextual innovativeness, virtual communities are essentially a priority area and a separate powerful field of study both in the space of national security and in the space of information culture.

Online videogames have provided and continue to provide the foundation for the study of virtual communities, namely online gaming communities, which are among the most representative online communities. In the framework of such analysis, the issue of identity is studied in particular, because the relationship between the videogame and the player gives rise to three different identities that are interconnected and have a mutual influence on each other:

1) a real person, i.e. the identity of the player in the real world, which does not disappear during the game, but, on the contrary, affects the choices and decisions made during the game;
2) virtual character, i.e. the identity that the player accepts as a virtual character in the virtual game world, usually represented by a certain "avatar" of the player;
3) projective identity, intermediate identity, which is a kind of "mediator" between the real identity and the virtual character.

According to the outlined levels of identity, there are two levels of virtual communities formed on the basis of video games:

1) Game community, i.e. a community of game characters who interact in the game world with other characters, build cities, fight NPS, kill monsters and common enemies, each other, and so on.
2) A community of players, i.e. a community of real people who interact with other people interested in the same game; these communities are very popular and active, and they are functional in relation to the game itself, because they can influence the game and modify the game environment, build new objects, create a new space that can be integrated into the virtual world of the game [31].

Most of all, the social interaction as the study of virtual communities through video games is noticeable within the so-called MMOs. MMOs – Massively Multiplayer Online Games – are videogames that are played on a console or PC, where hundreds, thousands or millions of players interact with each other in a stable online space that continues to exist even when a single player is not playing. These games can belong to many genres, from science fiction to fantasy role-playing games. MMOs provide a high social experience in which players not only compete but also

cooperate to achieve a common goal, talk to each other (via text or voice chat), exchange items or virtual currency and negotiate the distribution of rewards [32]. MMOs have contributed to the formation of the main array of virtual communities of players, because in other genres of videogames, social interaction is not so large and does not appear to be key to the ability to play a particular videogame. The infrastructure formed within other genres of videogames also does not provide such an opportunity to develop global interaction between players.

The digital online space has the potential to increase the level of social interaction, as opposed to the assertion of promoting social isolation. Games function as both culture and cultural objects, appearing as a so-called "window" into how different social structures influence individual and social behavior online [33]. However, this can also pose a threat because both these communities can be involved into terrorism, manipulations by enemies. It is difficult to trace the communication inside the game community because the videogame can be hosted on the servers of the enemy state; in some videogames, in-game chats are not recorded, so, they can be the place for communication that violates the state's law. Even communities created from videogame players can have anti-state nature and be formed to undermine the stability of some state and even several real states, because most videogames are accessible from different parts of the world.

Although videogames are the potential threat for cybersecurity, they can also be used to improve the security and solve different problems in this area. For example, the use of videogames as a means of improvement of authentication systems is proposed considering the possible transformation of password-choosing to the game in which the winning condition is creation the strongest password. The possible gamified system is shown as a game that proposes players to evolve mascots through the improvement of their password [34].

Videogames can act as a means of increasing the understanding of cyberspace and strengthening the cybersecurity of an individual. Researchers propose to increase cybersecurity awareness through VR-games designed to deepen knowledge about information flows, codes, cryptography etc., videogame trainings to combat malware [35]. Thus, videogames can be not only harmful, but also helpful for defending the state from cyber-threats.

4. Conclusions

Today, the question of cybersecurity is especially relevant due to the global nature and growing number of possible threats. Videogames, which are a specific part of cyberspace, can pose different threats and be used to manipulate people from other states, undermining these states' stability and peace. Consisting of different levels, videogames can be dangerous as a vulnerable software, which becomes a tool for fraud; as the media with the specific content; as the space for creation of dangerous virtual communities. Many videogames are global and it is difficult to cope with dangers that arise from their spread. All mentioned levels have their specifics and should be considered in detail, however, in scientific discourse, they are usually studied separately, without comprehensive view on videogames as a three-level object that can be dangerous for the state cybersecurity. In addition, one videogame can be a threat on all three levels. It is especially relevant when we talk about MMOs, which can be used for violation of laws on the level of the game system, can spread propaganda and stereotypes and form virtual communities aimed at terrorism and manipulations. However, even videogames which are used for entertainment can become a means of spying, stealing information and doing harm to the other state.

At the same time, videogames can be means of strengthening the cybersecurity. Through their use, the cybersecurity awareness can be increased, and individuals can be trained to combat malware. Videogames can also be used in strengthening such systems as authentication system, which can have positive impact on the secureness of the Internet in general.

Each of mentioned levels of possible threat of videogames in cyberspace should be considered furtherly, as well as tools to protect state cybersecurity from these threats and to make videogames less vulnerable should be developed.

References

[1] Malyk, Ya.: *Economic Security of Ukraine: Internal and External Factors*. Lviv, 202 p. (2002) (in Ukrainian)

[2] Al-Azawi, R., Al-Faliti, F., Al-Blushi, M.: *Educational gamification vs. game-based learning: Comparative study*. International Journal of Innovation, Management and Technology, 7(4), pp. 131-136 (2016). https://doi.org/10.18178/ijimt.2016.7.4.659

[3] Zhu, L.: *The psychology behind video games during COVID-19 pandemic: A case study of Animal Crossing: New Horizons*. Human Behavior & Emerging Technologies, 3, pp. 157-159 (2021) DOI: https://doi.org/10.1002/hbe2.221

[4] Aarseth, E.: *Playing Research: Methodological approaches to game analysis.* In Proceedings of Digital Arts and Culture Conference (Melbourne, May 2003) (2003). DOI: 10.7238/a.v0i7.763

[5] Craigen, D., Diakun-Thibault, N., & Purse, R.: *Defining Cybersecurity*. Technology Innovation Management Review, 4(10), pp. 13-21 (2014). http://doi.org/10.22215/timreview/835

[6] Renaud, K., Zimmermann, V., Schürmann, T., Böhm, C.: *Exploring cybersecurity-related emotions and finding that they are challenging to measure*. Palgrave Communications, 8, (1), pp. 1-17 (2021).

[7] Kuchta, B., Romaniuk, A.: *The Bases of Political Science*. Part 1: From the History of Political Thought from the

Ancient Time to Nowadays, pp. 26-27. Lviv: Kalvaria (1997) (in Ukrainian).
[8] Spinoza, B.: *The Collected Works in 2 Volumes*, V.2 Moscow: Thought, 311 p. (1957). (in Russian)
[9] Rousseau, J-J.: *The Social Contract.* Moscow: Thought, 171 p. (1969). (in Russian)
[10] Bryant, R.: *What kind of space is cyberspace?* Minerva - An Internet Journal of Philosophy, 5 (1) (2001).
[11] Determann, L., Guttenberg, K. T.: *On War and Peace in Cyberspace – Security, Privacy, Jurisdiction*. 41 Hastings Const. L.Q. 875 (2014).
[12] Bergonse, R.: *Fifty Years on, What Exactly is a Videogame? An Essentialistic Definitional Approach*. The Computer Games Journal, 6, 10, pp. 239-255 (2017). DOI: 10.1007/s40869-017-0045-4
[13] Caillois, R.: *Man, Play, and Games*. University of Illinois Press (2001).
[14] Frasca, G.: Ludology Meets Narratology: Similitude and differences between (video)games and narrative (1999). Retrieved from: https://ludology.typepad.com/weblog/articles/ludology.htm
[15] Horban, O., Martych, R., Maletska, M.: *Phenomenon of Videogame Culture in Modern Society*. Studia Warmińskie, 56, pp. 123-135 (2019). https://doi.org/10.31648/sw.4314
[16] Konzack, L.: *Computer Game Criticism: A Method for Computer Game Analysis*. In Computer Games and Digital Cultures Conference Proceedings, pp. 89-100. Tampere University Press, June, 2002 (2002).
[17] Salen, K., Zimmerman, E.: *Rules of Play: Game Design Fundamentals*. Cambridge MA: MIT Press Visual Communication (2003).
[18] Djaouti, D., Alvarez, J., Jessel, J-P.: *A gameplay definition through videogame classification*. International Journal of Computer Games Technology. Vol. 2008. (2008).
[19] Pontiroli, S.: The Cake is a Lie! Uncovering The Secret World of Malware-Like Cheats in Video Games. In VB2019, London, 2-4 October, 2019 (2019). Retrieved from: https://www.virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Pontiroli.pdf
[20] Bardzell, J., Jakobsson, M., Bardzell, S., Pace, T., Odom, W., Houssian, A.: *Virtual worlds and fraud: Approaching cybersecurity in Massively Multiplayer Online Games*. Paper presented at 3rd Digital Games Research Association International Conference: "Situated Play", DiGRA 2007, pp. 742-751. Tokyo, Japan. (2007).
[21] Hemenover S.H., Bowman, N.D.: Video games, emotion, and emotion regulation: expanding the scope. Annals of the International Communication Association, 42:2, pp. 125-143 (2018). DOI: 10.1080/23808985.2018.1442239
[22] Andiloro, A.: *Uncovering propaganda in war videogames*. Two year's Master's Thesis, Programming, Department of Informatics and Media, Uppsala Universitet (2017).
[23] Lippmann, W.: Public opinion. Harcourt, Brace (1922).
[24] Formosa, P., Ryan, M., Staines, D.: *Papers, Please and the systemic approach to engaging ethical expertise in videogames*. Ethics and Information Technology. 18 (3), pp. 211-225 (2016).
[25] Jarvis, L., Robinson, N. War, time, and military videogames: heterogeneities and critical potential, Critical Military Studies, 7:2, 192-211, DOI: 10.1080/23337486.2019.1573014
[26] Nick Robinson (2019) Military Videogames, The RUSI Journal, 164:4, 10-21, DOI: 10.1080/03071847.2019.1659607
[27] Astafeva, O. N.: Synergetic approach to the study of socio-cultural processes: opportunities and limits. Moscow: RAGS, 316 pp. (2002). (in Russian)
[28] Dziundziuk, V. B. Virtual Communities: a Potential Threat to National Security. State building (2011). (in Ukrainian)
[29] Aleksandrova, O., Khrypko, S.: *Solitude as a Problem of Human's Mature Choice*. Beytulhikme. An International of Philosophy, 10(3), p. 771-785 (2020). https://doi.org/10.18491/beytulhikme.1582
[30] Khrypko, S. Iatsenko, G.: *Philosophy of a Name: Ukrainian Context*. Beytulhikme An International Journal of Philosophy, 9 (2), p. 437-451 (2019).
[31] Tardini, S., Cantoni, L.: *Development of IT and Virtual Communities*. In Encyclopedia of Multimedia Technology and Networking, Edited by M. Pagani. Hershey-New York: Information Science Reference, p. 349-355 (2009).
[32] Croft, J.: "It's just a game": *Ethical reasoning within virtual worlds*. GoodWork Project Report Series, 73 (2011). URL: https://static1.squarespace.com/static/5c5b569c01232cccdc227b9c/t/5e8de2e3ce118367c46962cb/1586356963462/73-Its-Just-a-Game.pdf
[33] McCauley, B., Nguyen, Truc Ha Thanh, McDonald, M.: *Wearing S. Digital gaming culture in Vietnam: an exploratory study*. Leisure Studies, 39:3. pp. 372-386 (2020). DOI: 10.1080/02614367.2020.1731842
[34] Kroeze, C., Olivier, M. S.: *Gamifying authentication*. Information Security for South Africa, 2012, pp. 1-8 (2012). doi: 10.1109/ISSA.2012.6320439.
[35] Moon, T., Abegaz, T., Payne, B., Salimi, A.: *MalAware Defensive: A Game to Train Users to Combat Malware*. Journal of Cybersecurity Education, Research and Practice, Vol. 2020: No. 1, Article 2. (2020)

1. Levyk Bogdan is Doctor of Historical Sciences, Senior Scientists, Director of Regional Scientific and Educational Center "Holodomor, Holocaust, International Dialogue", Lviv Polytechnic National University, Lviv, Ukraine. His research interest includes information security, security of virtual communities, security studies, military security
ORCID: http://orcid.org/0000-0001-5100-0834

2. Mariia Maletska received the B.E. and M.E. degrees, from Borys Grinchenko Kyiv University. in 2019 and 2021, respectively. She has been a research assistant at Borys Grinchenko Kyiv University since 2016. Her research interest includes videogame philosophy, game studies, social philosophy and philosophy of education.
ORCID: https://orcid.org/0000-0003-3123-9500

3.Svitlana Khrypko received the B.E., M. E., and Cand. of. Philosophy degrees. She has been an associate professor at Department of Philosophy, Faculty of History and Philosophy, Borys Grinchenko Kyiv University since 2018. Her research interest includes axiology, culturological studies, ethnic studies, philosophy of education. multiculturalism of virtual communities.
ORCID: https://orcid.org/0000-0001-9426-4549

4. **Kryvyzyuk Leonid** is Candidate of Historical Sciences, Assistant Professor, Department of Military Intelligence, Analysis and Prognosis of Socio-Political Processes, Hetman Petro Sahaidachnyi National Army Academy. His research interest includes information security, security of virtual communities, security studies, military security
ORCID: 0000-0001-9094-4061

5. **Dobrodum Olga** is Doctor of Philosophical Science, Professor, Professor of the Department of Culturology and Philosophical Anthropology of the National Pedagogical Dragomanov University. Her research interest includes political security, geopolitical context of security studies
ORCID: http://orcid.org/0000-0001-7651-4946

6. **Katerina Pasko is** Candidate of Philosophical Sciences, the Associate Professor of the Department of Psychology Educational-Scientific Institute of Pedagogy and Psychology of Sumy State Pedagogical University named after A.S. Makarenko. Her research interest includes
ORCID: https://orcid.org/0000-0003-0488-9719