UDC 101

SOCIOCULTURAL ANALYSIS OF CYBERTERRORISM IN SOCIAL NETS WITHIN THE PROBLEMS OF INFORMATION SAFETY OF RUSSIAN SOCIETY

E.E. Nesmeyanov, A.M. Rudenko, V.V. Kotlyarova

Don state technical university. Rostov-on-Don, Russia.
nesmeyanoff.e@yandex.ru, biktoria66@mail.ru, amrudenko@list.ru

An attempt of the socio-cultural analysis of the problem of cyber-terrorism in the social networks has been done. The authors argue that, despite a number of positive features of communication that in contemporary Russian society operate social networks around the world, they are increasingly becoming a source of massive attacks of cyberterrorism, perpetrated with the aim at harming human life and society. It is argued that cyber-terrorism, initially hiding under the guise of social and active user on the network, eventually leaving the virtual space becomes a real manifestation of terrorism.

Key words: safety, information safety, cyber terrorism, social network, Russian society.

In the modern social and the humanities knowledge it is updated research questions of socio-cultural phenomena, processes and objects in terms of their security settings. Subject field research data are gradually expanding. In the third millennium of science it has been a surge of attention to various aspects of the safety of man and society - political, informational, technological, economic, military, environmental, cultural, humanitarian and other.

One of the main aspects of human security, and society as a whole is counter-terrorism. Unfortunately, in today's world geopolitical ambitions of individual states create conditions for violent content conflicts that provoke terrorism. On the other hand, the destructive separatist forces or national-patriotic movement, considering and using these ambitions, resorted to terrorist methods to achieve their goals by applying, in particular, and information and communication technologies.

Modern society is inconceivable without information technology, substantially transformed not only the forms and principles of processing and transmission of information, but also provide a powerful impact on the socio-cultural, economic, political, military and strategic aspects of public life. It is no accident today observed that "... the global world, unfortunately, is increasingly becoming a space in which the information war" [11, p. 635]. The revolution in information technology, started at the end of last century and covers all areas of human activity, is gradually transforming the modern world in the context of the formation of its new network structure of the sample. Today informatization as the process through increased global processes in all regions of the world not only provides access to all categories of members of modern society to the information resources, but also contributes to their active participation not only in information exchanges on a massive development processes of information creation, but also promotes the involvement of information and an active part of society to participate in terrorist activities. Contoured range of problems determines the relevance of the topic, causing the purpose of this article - conducting socio-cultural analysis of the problem of cyber-terrorism.

It should be noted that in scientific publications devoted to this subject is actively highlighted the problem of the information security community. Several publications domestic and foreign scientists devoted to the problems of the theoretical study of the information society: A. Toffler, S.P. Rastorguev, G.G. Pocheptsov [9], A.V. Nazarchuk [8, p. 61-75]. The phenomenon of social networking since the mid 90s of the twentieth century attracted attention of researchers. A.V. Arshinov, Y. Danilov, V.A. Tarasenko consider synergistic aspects of the social networks, the problem of communicative interaction are considered in the works of P.K. Zaleski, I.A. Gronskii [3]. Special contribution to the discussion of the problem of philosophical studies of social networks have made the study of M. Castells. In his trilogy "The Information Age: Economy, Society and Culture" (1996) was the first social networks are considered as the basis for a new type of society that meets the information age in human development - network. The researcher interprets the new type of social structure through the concept of "network society", "because it created networks of production, power and experience that form the culture of virtuality in the global flows of cross time and space" [5, P. 505].

Traditionally, a modern system of social and humanities and social networking phenomenon of cyber-terrorism (as well as any other element of social reality) is proposed to analyze the positions of the different methodological approaches (historical, regulatory, institutional, structural and others). However, in our view, given the peculiarities of the process of formation of modern social networks, namely their direct participation in the formation of a new kind of culture - the culture of real virtuality, will be the most appropriate in their study, the dominant role is given to the sociocultural approach. It is obvious that "in the application of socio-scientific aspects of sociocultural approach are considered and the two interconnected tendencies of socio-cultural changes - the institutionalization carried out by certain socio-cultural mechanisms, and the universalization of the process of disclosure of the essential powers and abilities and powers of man, realized in antroposotsiogeneza [10, P. 307].

The first concerns the possible consequences of the use of the World Wide Web as a base for terrorist attacks was proposed in 1993 futurologist A. Toffler in "The Metamorphosis of Power" when the general public has little knowledge about the Internet: "As we move further into a period of rapid economic and political development of the irregularly intermittent technological achievements and disasters, we can expect that the crisis will follow one another - from terrorist attacks and sudden decline in production to international crises" [13, p. 237]. A. Toffler already predicted that terrorists would try to carry out blow to the information and telecommunication infrastructure of the United States. Currently, experts' opinions on the new concept of "cyberterrorism" diametrically divided. The first sounding the alarm about the potential dangers of cyber war, others, usually in scientific work, regularly remind the first so far in the world has been no cyberterroristic act. By the conclusion reached in the report "Cyberterrorism: myth or reality?" S. Thévenoz: "If art Information Piracy frankly worded as engineering academies, universities, discussed at the workshops by local and international experts on defense issues ... then cyberterrorism in the strict sense of the word, does not exist and still "[4, p. 45]. However, serious cause for concern is still there. In the history of the Internet, there are precedents for the destruction of the political objectives of the start pages of Web sites (such as the military or the government). Known and cyber attacks aimed at overloading the servers and block access to them.

Human activities on the Internet can act as the five major forms isolated expert American Studies Center Terrorism D. Dennig: collection, publication, dialogue, coordination and direct lobbying of decision-makers. According to D. Denning, the Internet is now considered a powerful lever for change of course domestic and foreign policy of any state, and in this aspect involves three activities: social activism, hacktivism and cyberterrorism. [15]

The first kind of human activity - social activity - does not provide for any terrorist activity, and is in various forms of expression. Forms may be different: creation of sites, sending emails, writing electronic publications, discussion of problems, creating a certain coalitions in forums and chat rooms, the organization of activities of the latter.

The second category is socially active Internet users involve mostly illegal methods of work. Their actions vary within the offense-a crime, but a malfunction of certain sections of the network, caused by these actions do not cause significant damage. Examples - strike on the Internet, targeted bombing whose e-mail, web hacking, computer breaks, viruses and "worms."

Hacktivism - a combination of social activism and hacking. People use specialized software. The vast majority of socially active hackers seeks to both can be better informed about its activities. Strikes on the Internet by hackers are to visit a particular site and the creation of such traffic, in which other users can not visit this site.

Bombing email undertaken hacktivists, also called "swarming" (from the English. - Swarming). One thing two or three letters to e-mail, providing feedback. Another thing - a thousand or thousands of letters sent simultaneously with the help of special programs: the mailbox is full, other visitors can not contact with the owner. Computer viruses and "worms" used by hacktivists tend to spread message of containing protest calls and damage software or computer can cause physical harm (reprogram it to self-destruction). The first protest related to the computer "worm" and characterized as cyber-terrorism, occurred in 1989 Scientists Administration National Aeronautics and Space United States saw the picture with the inscription: "Worms Against Nuclear murderers! You talk about peace for all, and are ready for war. " Thus, the protesters demanded to stop the launch of the space shuttle to Jupiter with the equipment powered by radioactive plutonium.

The term "cyber terrorism" is not a precise definition. Among theorists and practitioners continued discussion on this subject. Successful seems to us the definition proposed Klaem B. (USA) [14]. Cyber-terrorism - is the use of computers as a weapon of politically motivated international or national groups or clandestine agents, which cause or threaten to cause harm or to cause panic, to influence the public or the government to change policy. We add that the aim of cyber-terrorists may be political and economic destabilization, sabotage, assigning military and civilian assets for political purposes, scrapping of computer networks, cyberwar and the like.

Modern cyber terrorism is trying to hide under the guise of social and active user of the network, while leaving the virtual space of cyber-terrorism and appears in terrible guise of modern terrorism. Today, terrorists are actively using the Internet to disseminate their propaganda on websites, forums, and in the form of videos, especially to report their successes and attract supporters. For example, a form of informational influence actively resorted militants LIH (banned terrorist organization in the Russian Federation).

What is the reason for the overwhelming success of terrorist organizations in the space of the Internet, including social networks? In our opinion this is due to the change of culture and ontological bases, respectively, with the change of personal identification of the person in it. Information technologies contribute to the growth of social activity in society. This activity is expressed in the opportunities for self-expression, sharing their own experiences. This is especially true when using social networking technologies. According to M. Castells, one of the leading specialists in the field of network community, the material basis of the new culture becomes "timeless time" and "space of flows". In the information society, culture is the culture of virtual reality, positioning the virtual, imaginary world as its ontological basis [5, p. 375].

Modern social networks should be seen not simply as a series of sequential discoveries of certain social projects individuals or groups in different countries (for example, «Facebook» (in October 2003 M. Zuckerberg in the US), "Classmates" (March 2006 A. Popkov in the UK), "VKontakte" (June 2006 P. Durov in Russia), etc.), but also as a certain way structured education formed the development of computer and telecommunication technologies. In social networks formed an idea of the congruence of the real world, but in the "virtual reality" processes are special rules set by the user. Some anthropological approach allows us to analyze social networks, primarily as a mechanism (a set of institutions) with which the person has an opportunity to better deal with the specific problems of their life; a system of different types of activities, each of which is a means of satisfying certain human needs and achieve its objectives; integral whole, all the elements (agents, relationships, resources) which are present in the organic relationship and ongoing dynamics.

That is why social networking is not nameable had to be (in one way or another version), because According to a representative of the German philosophical anthropology A. Gehlen, man is inherently a social being, "because there is no point in talking about the" environment "as applied to him because he lives in the world of culture, defines its adaptation to virtually any terrestrial environment, regardless of climate" [12, p. 43]. And further, "a man - says German philosopher - does not know who and what he is, but because it can not itself implement directly, it must organize itself institutions" [12, p. 74].

Modern technologies have the ability to influence the information; modern technologies tend to the effect of "universal influence"; all systems using information technology, are subject to "network logic", which allows them to influence a number of processes and organizations ("the topological configuration, according to M. Castells - network - can now, thanks to new information technology material provided in all kinds of processes and organizations "[5, p. 77]. Network technologies are flexible, allowing them to constantly change and adapt, the new information technologies converging at a high speed in a highly integrated system.

Among the large variety of information technologizing influence as the main method of distributing allocated specially selected information (disinformation). Disinformation is presented in the form of e-mailing, organizing, and differentiation of groups in social networks (with the same interests, on the news, etc.), posting private information on public Internet sites, the creation of special sites with elements pseudointeractive communicate their visitors, etc.

In social networks very actively used manipulative techniques. Part of the application of these technologies was discussed in our previous publications [7, p 622 - 625; 11, p 635 - 638]. However, the most "productive" ways for cyber attacks on social networks are the suggestive technology, purchasing scale, correlated with a military threat to national security [1]. Such techniques are particularly effective in the Internet for specific reasons. There is still a high degree of public confidence in the unofficial sources of information. Audience takes place by unrealistic promises to solve any problems. Also, online communities are often formed on the basis of empathy. Technologization user interaction in social networks brings new adjustments in view of the information security of the person and of society. Personal data of users are in the public domain may be used without permission for advertising purposes, through the fault of the network can be carried leak billing, etc.

Information, exercising a regulating effect on the behavior of people through the formation of worldviews, may distort the true aims, interests and needs. As we noted earlier, "hyperspace new virtual reality constructed a global communication network, there is a threat of losing their collective person and, as a result, personal identity" [6]. In this case, the virtual environment has a negative impact on the decisions made, can contain a great potential of destruction in its content represent implicit and explicit threat to the existence of social systems: the individual, society and state.

Thus, the analysis of the existing social experience shows that social networks, with the available resources of social trust, successfully applied for the promotion of a number of subjects of interest to the effect of the introduction of information into the public circulation of certain information. They are individual users and society as a whole may be affected by this distorted information, becoming one of the main tools of modern terrorists. In this aspect, the very revealing example, when the Egyptian Google top manager Wael Ghonim asked what country after Egypt to start the next revolution, advises, "Ask Facebook» [2]. In this regard, G.G. Pocheptsov said: "Communication is the most effective way to make changes in this world. Therefore, it will stand at the center of all the changes. As the book changed structure of the world, so the Internet to do the same. He built a new map of the world, where the starting point would be virtual rather than physical reality" [9, p. 19]. Social networks, despite the fact that in everyday practice has recently entered, have become an important technology not only to the organization of social protests that contribute to the improvement of society, but also destructive performances for solving purposes not related to national progress. That social networks in the modern world are increasingly becoming a source of massive attacks of cyberterrorism, done with the aim to cause serious damage to human life and society in order to overthrow the government and establish a new political regime.

References

1. Ahidzhakova M. Linguistic suggestive funds as one of the ways to influence the mass audience. Access: http://window.edu.ru/window_catalog/files/ r60798 / lang_1.pdf.
2. Voloshin V. About the revolution in Egypt via Facebook [Electronic resource] // Komsomolskaya Pravda. Access: http://www.kp.ru/daily/25637/801883/

3. Gronskii I.A. Social and philosophical foundations of the activity of the Internet audience in the network communication: the Abstract of the candidate of philosophical sciences. Nizhny Novgorod, 2011.
4. Inozemtsev V.L., Kuznetsova E.S. Atlas 2010 Le monde diplomatique. M., 2010.
5. Castells M. The Information Age: Economy, Society and Culture / Manuel Castells; [trans. from English. under the scientific. Ed. AI Shkaratan]. M., 2000.
6. Kotlyarova V.V. Sources of threats in the virtual environment: the transformation of the living space of the person [Electronic resource] // APRIORI. Series: Humanities. 2015. No 6. http://apriori-journal.ru/seria1/6-2015/Kotlyarova.pdf
7. Kotlyarova V.V. The phenomenon of terrorism information: axiological aspects // Young scientist. 2015. No 14 (94).
8. Nazarchuk A.V. Network society and its philosophical interpretation. Problems of Philosophy. 2008. No 7.
9. Pocheptsov G.G. Information wars. The new policy instrument. M., 2015.
10. Reznik Y.M. Socio-cultural approach as the research methodology / YM Resnick // Questions of social theory. 2008. Volume II. Vol. 12.
11. Rudenko A.M., Shestakov Y.The problem of manipulating the mass consciousness as a factor of destabilization of the information security of modern Russian society // The young scientist. 2015. No 14.
12. Rutkiewicz A.M. A. Gehlen's theory of institutions // History of Philosophy. M., 2000. No 5.
13. Toffler E. Metamorphosis of Power: Trans. from English / A. Toffler. M., 2003.
14. Clay W. Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress [electronic resource] // fpc.state.gov> documents / organization / 45184.pdf
15. Denning D. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy by [electronic resource] // http://www.cs.georgetown.edu/~denning

November, 17, 2015