IRSTI 21.01.29 DOI: https://doi.org/10.26577//EJRS.2021.v27.i3.r7

M. Abdullaeva

International Islamic Academy of Uzbekistan, Uzbekistan, Tashkent,
e-mail: mirzohira@mail.ru

CYBERJIHAD: EXPRESSIONS OF TERRORISM ON THE INTERNET

The Internet, along with its public promotion, has developed into the integrator of cultures, a means of communication between business, consumer and government. However, as the volume of users increased, cases of its utilization different from its initial purpose increased, too. Namely these are pornography, content promoting violence, as well as an influence of various extremistic organizations. Groups pursuing various political goals commenced to use the network to carry out their own propaganda, to communicate with their supporters, to raise public awareness of what they are doing, and even to carry out their own opreations by the virtue of the internet. The article provides conclusions and suggestions on cyberjihad and cyberterrorism, which take place in cyberspace, on the basis of scientific approaches to them. Some thoughts and summaries are provided here to highlight the use of the term Islam as well as the essence of the word "jihad", which derived from the Arabic language. The methods of comparison and germenetic analysis were used in carrying out the study.

Key words: cyberspace, internet, cyber terrorism, information society, physiological war.

М. Абдуллаева

Өзбекстан халықаралық ислам академиясы, Өзбекстан, Ташкент қ.
e-mail: mirzohira@mail.ru

Кибержихад: ғаламтордағы терроризмнің көрінісі

Бүгінгі күнде ғаламтор желісі адамдар арасында жылдам насихатталумен, жаппай қолданылумен қатар, мәдениеттің интеграторына айналып та үлгерді, бұл дегеніміз бизнес, тұтынушы мен үкімет арасындағы байланыс құралы. Алайда, қолданушылардың саны артқан сайын, оны бастапқы мақсатында қолданудан ауытқу жағдайлары да өсе түсті. Атап айтқанда, бұл қатарда порнография, зорлық-зомбылықты жаппай насихаттайтын контентті қамтыды, сондай-ақ әр түрлі экстремистік, террористік ұйымдардың көздеген жасырын мақсаттарының әсері де болды. Әр түрлі жасырын, саяси мақсаттарға ұмтылған топтар бұл желіні өздерінің үгіт-насихат немесе байланыс құралы сипатындағы жұмыстарын жүргізуге, өз тараптастары, жақтастарымен қарым-қатынасқа түсуге, не істеп жатқандары туралы жұртшылықты хабардар етуге, тіпті интернеттің көмегімен өз істерін жүзеге асыруға қолдана бастады. Сондай-ақ, мақалада киберкеңістікте орын алып жатқан кибержихад пен кибертерроризм бойынша оларға ғылыми көзқарастар негізінде қорытындылар мен ұсыныстар берілген. Мұнда ислам терминінің дұрыс қолданылуы және араб тілінен алынған «жиһад» сөзінің мәнін айқындау үшін кейбір ойлар мен қысқаша мәліметтер берілген. Зерттеуді жүргізу, көзделген мақсатқа, нәтижеге жету барысында салыстыру мен герменевтикалық талдау әдістері қолданылды.

Түйін сөздер: киберкеңістік, интернет, кибертерроризм, ақпараттық қоғам, физиологиялық соғыс.

М. Абдуллаева

Международная Исламская Академия Узбекистана, Узбекистан, г. Ташкент,
e-mail: mirzohira@mail.ru

Киберджихад: выражения терроризма в интернете

На сегодняшний день сеть Интернет, наряду с быстрой пропагандой и массовым использованием среди людей, уже стала интегратором культуры, а значит, средством коммуникации между бизнесом, потребителем и правительством. Однако, по мере увеличения числа пользователей увеличивались и случаи отклонения от его первоначального использования. В частности, это включало в себя порнографию, контент, пропагандирующий насилие, а также влияние скрытых целей, преследуемых различными экстремистскими, террористическими организациями. Группы, преследующие различные скрытые, политические цели, стали использовать эту сеть для ведения своей пропагандистской или коммуникационной работы, общения со своими сторонниками, информирования общественности о том, что они делают, и даже для осуществления своей деятельности с помощью Интернета. В статье также приводятся выводы и рекомендации по происходящему в киберпространстве киберджихаду и кибертерроризму на основе научных подходов к ним. Дается краткое изложение правильного использования термина «ислам» и значение слова «джихад» арабского происхождения. При проведении исследования, достижении намеченной цели, результата использовались методы сравнения и герменевтического анализа.

Ключевые слова: киберпространство, Интернет, кибертерроризм, информационное общество, физиологическая война.

Introduction

The network, which was used for academic purposes by interconnecting computers in the 1970s, changed its character 20 years later and spread widely. More than 18,000 private, public and national networks were connected to each-other by this network in the mid-1990s. 3.2 million head computers along with 60 million users from developed countries were connected to these networks. According to the approximate calculations carried in the beginning of the XXI century, their number has increased by more than a billion.

The opportunities such as easy communication, lack of rules, large audience coverage, speed of data flow have led the Internet to become a lightweight way of achieving the goals of those who commit terrorist acts that threaten the society.

These advantages did not go unnoticed by terrorist organizations, regardless of their political purpose. Terrorist organizations operating in different points of the world have united in a single global network.

Justification of the choice of articles and goals and objectives

The term cyber jihad is one of the new in Religious Studies. However, studing them and using it in a scientific literatures gives an opportunity to separate reality from delusion it. The article anylyses the orthodox meaning of jihad and transformation it to cyberspace. For this reason, it was chosen as a object term “jihad” and “cyberjihad”.

Scientific research methodology

Since the cyber jihad is considered as relatively new term in scientific discussions, the studies in this regard hardly exist in uzbek language. nevertheless, the classical aspects of the issue have been comprehensively studied by a number of scientists and researchers, namely, Muradov (2019); Uvatov (2002); Komilov, Khasanbaev (2009); Zakrulaev (2010); Giyibnazarov (2013); Savelova (2018); Betanov (2018), Onwudiwe (2018); Alexander (2019); Ivanov (2019). Also, terrorism is not a new subject of scientific research. Moreover, terrorism is far from new subject of scientific investigations. The study of their content, essence, properties and appearance occupies a significant part in researches of representatives from the relevant field. Terrorism has become an object of scientific research since the time of the great french revolution (Manferd, 1989:351). The main accent in such researches was put on the analysis of history of extremism and terrorism and their aspects related to spirituality and religion (Abduhamidov, 2018; Umarov, 2018; Rahimjonov, 2019).

From the second half of the 1990s, there have been observed even more intensive public functioning of religious organizations in cyberspace. During this process, diverse organizations also promote their own political goals by means of masquerading as religion organizations with respective purposes through web pages on the internet (Surma, 2016:40; Seed, 2019; Vacca, 2019; Osman K., Alarood A., Jano Z., Ahmad R., Manaf A., & Mahmoud M. 2019; Topal R. 2019). In this regard, it should be noted that the prime task of the “internet space” doesn’t only consist of providing information about the activities of this or that social institution, but also includes a utilizing of new technologies on the basis of the unification of people of traditional religions.

An analysis of the cyberjihad phenomenon in geopolitics, calling on cyberjihad to carry out consumer activity as well as terrorist activities on the web, studies have been conducted by Western scientists as a virtual war. The methods of comparison, generalization and germenetic analysis were used, in this article.

Results and discussion

Cyberjihad and cyberterrorism’s interpretation.

For a broader understanding of the cyberjihad process, it is necessary to properly understand its interpretation in Islam. “Jihad” – (Arabic. “enthusiasm”,” “employing power”) means “serious effort”, which means that a person does his best in order to achieve his goal (Zhaholatga qarshi ma’rifat, 2019: 33). In terminology, however, this word is used in many meanings. In particular, there are such types of “jihad” as: calling to the way of Allah, calling for virtue and preventing from doing evil, the struggle of a person against his own desires in the way of Allah, serving to parents.

The following hadith narrated from Imam Termeziy, which says:” the excuse of Jihad is that man must strive against his own self as Allah Almighty pleases” can be considered as an evidence for this. In addition, Imam Bukhari and Imam Muslim have narrated: “one person approached to the messenger of Allah and said:” I want to participate in jihad.” Then the messenger of Allah asked if he has parents. “Yes,” he replied. Then messenger of Allah said, “ go attend them and help, do your service! “This is going to be your jihad,” the messenger said. Thus muslim elders claimed that the service an offspring does to its parents is equaled to jihad.

The word “jihad” isn’t translated as “war” in Arab dictionary but the word “qitol” carries the meaning of “war”. Jihad in Islam, first arose not in the sense of war, but in the sense of calling to the religion of Allah. Passionate desire overcoming it and striving to live in accordance with the Sharia, finding and saying the place of the true word, is also included in the World (Islamic Encyclopedia, 2017, p. 164).

So what cybersecurity means is to wage war in cyberspace using the latest digital technologies (Drobotenko, 2019, p. 27). The distinctiveness of the cyberjihad phenomenon is characterized by its complexity. It involves both technological and technical aspect. If the technological aspect masters the method of informational and psychological influence on human consciousness, the aspect of damaging infrastructures and causing serious technogenic accidents will be acquired. And the technical aspect makes it possible to carry out cyberterrorism.

Western media has been covering the subject of terrorism, in connection with violent extremism and sacred war, in recent years. The threat of the cyberterrorism covers media, security associations and information and communication technologies. The term cyberterrorism began to be used in the late 1980s as part of research on the potential risk of high technologies in the emerging “informatized society”, with increasing rates of internet use. At the beginning of the 90s, the National Academy of Sciences of the United States cited computer security reports that “tomorrow’s terrorist could inflict more horrific damage than a bomb just using computer keyboards.”

Dorothy Den, a professor of Computer Science, in the one of her various articles described cyberterrorism – as follows: “cybeterrrorism is a phenomenon that occurs at the crossroads of cybercrime and terrorism. An illegal attack on computers and network information aimed at forcing or intimidating a government or nation to achieve political or social objectives is understood to be dangerous. Furthermore, in order for the cyber-thread to be considered as terrorism, the degree to which fear arises must be an attack resulting from damage or violence on humans and property. Attacks that lead to human death or physical injury, as well as explosions and strong financial losses, can also be considered as cyberterrorism. Serious attacks on strategic objects can be considered a cyberrorism movement, too. Attacks, which do not prevent work to be carried on or have only a disturbing effect are not considered as cyberterrorism.

It is important to distinguish between cyberterrorism and “hacktivism” (a combination of the words hacker and activism) from each other in such cases. The “hacking” movement is an action aimed at exposing data, using vulnerabilities in computer operating systems or software and manipulating, both online and in secret. In contrast to hacktivists, hackers do not usually have a political program. Primarily, hackers have four types of weapons in their arsenal: virtual blockade (blockade); attack on e-mails; hacking on the site and computers; computer viruses.

Virtual blockade (siege) is a virtual form of the physical blockade. Complaintents generalize the traffic of the site to this extent, so that another user can not have an access to this site. “Swarming” if there’s a great number of users approached the website at once, operating lags in this site occure. “ worm “also serves to increase the impact of the second type of weapons of the hacktivists: an attack on an email is also known as “ Ping – attack”, that is, sending thousands of letters at the same time.

Breaking into the site and computers – many cybercriminals use the third weapon of hacktivists. Computer systems should be disrupted in order to reveal the information, correspondence, financial reports and other files to carry out this process. We can observe that such crimes are annually increasing. For instance, according to the report of the Center of coordination group for Rapid Response to computer accidents, in 1997, the state of computer disruption encountered 2 134 times , in 2000, their number increased by 21 756 units, in 2003 by 137 000. These numbers show the rise in quantity cyberattacks and how the thousands of victims have become the object of simple and complex hacking machines.

The fourth weapon of the hacktivists involves viruses. Being in form of malicious strings of code they can damage computers and spread one computer to another via network.

Although, hacktivism is aimed at political goals, it isn't considered as cyberterrorism. Admittedly, hacktivists counteracts and disable hardwares, however, they don't aim to kill , hurt or frighten someone. Nevertheless, the hacktivism lifts the risk of cybertrorism to the first place. In addition, the border between cyberterrorism and hacktivism can sometimes be washed away. Particularly, hacktivists led by terroristic groups or vica versa, the hacktivists assistance to terrorists by enhancing their activity and attacking the strategically important infrastructure such as, electricity network and the emergency service, are the acts of cyberterrorism.

During the years 2003-2004, hundreds of sites serving or supporting terrorists were identified, while analyzing web sites on the internet (Weimann, 2004).

Ineternet terrorist-inspired websites quickly appear, change their format and disappear in a blink. In general, those disappeared web sites change their online address but keep the content.

According to the analysis of Professor Gabriel Weinman of the University of Haifa, terrorism inspired web sites target three types of audiences on their own (Weimann (a), 2004):

Current and potential supporters.

Web sites in the spirit of terrorism put great effort on the use of slogans and sell to their supporters various items, for example, T-shirts, emblems, badges, flags, videos and audios are also promoted by them. Usually such organizations try to "lure" local supporters into the bait through websites in that language. In addition, they post detailed information about their activities, about the internal policy of the organization, its supporters and enemies in those web sites.

International community opinion. The international community is not directly involved in these conflicts, but is interested in versions of the site different from the local language and their practice. From numerous content analyzes it is known that foreign journalists are also under their target. Often it's important indeed for foreign journalists to get a detailed information about the occured accident. Only one Hezbollah site offers journalists to collaborate with their press House via e-mail.

Contrary community. The access for public, which most oppose the content of the sites, is not clearly exposed. However, some sites try to demorilize the enemy by attacking him and evoking a sense of guilt. In such a process, they try to change the public opinion and "raise"it against the statements of those who oppose it.

Ways terrorists use the internet

Scientists have noted that there are eight ways that terrorists use the internet. These are:

Psychological war;

Promotion and propaganda;

Data collection;

Collecting money;

Recruitment and mobilization;

Sharing information;

Planning;

Agreement.

Terrorism is usually understood as a **psychological war**, so that terrorist planned to wage similar type of war. There are several ways for terrorists to lead such a war. For instance, they use the internet to spread false information, to organize an attack aimed to persuade people in their vulnerability, to disseminate pictures of corps of people who have been brutally killed, taken from their latest practices. Moreover, terrorists carry out a psychological offence , through cyber fear. An example of this is the formation of belief that terrorists in the public can come up with such a threat as committing a catastrophe through the dismissal of control in the air transport system or by attacking computers that regulate the national economy system.

As the possibilities of the Internet have increased, the possibilities of the popularity of terrorists have also expanded. Previously, they sought to attract the masses to their activities through the printing press, radio and television. However, they couldn't achieve their goals because of multi-layered. Today, every terroristic organization has managed to have websites that it disposes of. According to Professor G. Weinman, such sites usually use three types of rhetorical structure in justifying the violence perpetrated by the organization.

Firstly, terrorists declare that they have no other measures than to resort to violence. Terroristic organizations usually describe such cases as the brutal killing, limited freedom of speech and prisoning of their supporters. Thus, they display themselves as small, helpless organization which are victimized by a stronger state organization.

Secondly, the rhetorical structure is to legalize the use of this violence and thus to blame the opponent. So members of this movement or organization, position themselves fighters for liberty.

Thirdly. extensive use of the word in the rejection of the use of violent methods in the rhetorical structure. These terroristic organizations declare and call for peacefull solution and diplomatic negotiation by accepting their goals on these web sites.

They use multimedia technologies that embody ideological and practical recommendations within the **propaganda**, advertise, justify and interpret terrorist activities in the internet. Virtual texts, presentations, magazines, theoretical data, audio and video files, as well as electronic games created by terrorist organizations and their supporters can be examples of these.

The internet can also be interpreted as a large digital library. The world wide web itself offers billions of data pages today. The majority of these data is free. Such open data space will facilitate the collection of information for terrorists.

Terrorists have already turned to experts in the dissemination of propaganda and attacks through the Internet. However, while carrying cybercrime out, they try not to deteriorate network activity as much as possible, because the disruption in the internet is equal to the disruption in their own communication. According to experts K.Siaxari and J.Rollins, cyberattacks could be comprised of the following four areas:

loss of integrity, the information can be changed in the way it does not fit together;

Loss of connectivity. Here continuously processing information systems are modified to the extent that registered users cannot access them;

Loss of privacy, the disclosure of critical information for the unregistered user;

Material destruction, that is, information systems cease to function as planned as a result of material damage caused by different teams

In addition to using the internet to disseminate information and videos in an extremist spirit, it is also used as a directing force by secretly communicating with interested people who seems to have a tendency to such actions. The Internet forums, chat groups have become a strong global "soldier" reserve for terrorist organizations and their supporters.

Advices

Experts on combating terrorist activities in the Internet provide the following recommendations:

Dissemination of information on educational and behavioural content via the Internet in different languages, with the aim of exposing claims in the spirit of terrorism.

The more they use the internet for terrorist purposes, the more analytical data they provide to fight against themselves;

To create a healthy immune system in young generations on consuming of informational stream.

Along with the positive aspects, it is also necessary to be aware of the negative consequences of the use of informational stream. It is important to analyze the content and strategy of information, as well as to increase the culture of information consumption, in the increasingly globalized world.

The culture of information absorbtion refers to a system of knowledge, ability and qualification that lets receive, sort, understand and interpret information from the flow of information that serves human interests, fullness and the development of society. When it comes to information reception answer to the following questions should be found in order such a culture and skill to be nurtured

– Who transmits this information?

– Why is it transmitted in this way?

– What is the purpose of this information transfer?

The message that the formed culture of information absorbtion is contrary to our national interests and values, passes its specific shield role in relation to information. Therefore, the formation of rational and qualified use of the global information's opportunities in young people has a vital and practical importance today.

Even when it comes to the guidelines of the Islamic religion, it is required to examine and clarify it before believing in a transmitted message. In particular, in the 6-th verse of the Surah Hujurat of the Koran Karim the following statement is said: "O believers! If any one brings you a message, you must determine and examine it so that you do not regret what you have done by putting a burden on people who are in a state of ignorance!"

There's another verse of the Koran about this which also calls people not to follow the message and information received by various means blindly: "(O man!) Do not follow what you do not know exactly about! Because everyone will be responsible on each of the ears, eyes, hearts" (Isro, 36).

A few hadiths of the Prophet Muhammad are also narrated alike: " Allah checks the message, Satan makes a haste decision," is said. Also, there's another hadith narrated from Abu Huraira, where the messenger of Allah says: "To the fact that a person to speaks about everything he has heard is enough for him to be considered as a liar".

The person who acts according to information he heard but didn't check on whether it is true or not is equaled to a liar. This is because it creates the ground for the realization of the merciless goal of the one who is spreading the message.

Conclusion

From the comments above, we can conclude that in the fight against extremism and terrorism, special attention should be drawn to following aspects in the formation of ideological immunity in young people:

– Educate individuals to have an independent mind, a worldview formed on a healthy basis and a strong will. Educate young generations to distinguish between the various bads, create a sense of respect for national values and the immune response to influence of different religious streams by forming a healthy lifestyle in their hearts and minds

– to live constantly alert and considerate towards ideological threats, not to communicate with suspicious individuals who promise to teach the religion of Islam, avoid illegal published or prepared religious content, literature, disks, materials on mobile phones, sites that promote jihad, extremism, terrorism and missionary activities in the internet;

– promotion of a healthy lifestyle among young people, formation of their spiritual and moral education, implementing of efforts on the basis of cooperation of family-neighborhood-educational institution in the perfection of such great qualities as patriotism, humanism, kindness, in the minds of youth;

– to promote not to rush to directly receive and access to information on religious issues in today's realities of intensive exchange of information and not getting a prisoner of information offences;

– the formation of religious tolerance, respect for representatives of other nations.

– to prevent the emergence of negative perceptions and reflections about religion among the population in order people to apply to the representative of the Office of Muslims of Uzbekistan, local imams and specialists of the religious sphere with questions of faith, prayer and other religious issues.

Thus, the effectiveness of spiritual and educational propaganda in protecting against ideological attacks of various manifestations under the guise of religion should be increased in the 21st century, when the informational battle has intensified. The younger generation should be provided with in-depth analytical information about the positive changes taking place in our lives, their social activity should be improved. Thus, "the idea against the idea, the thought against the thought, the combat against ignorance with enlightenment" will play a vital role.

References

Abduhamidov, M. (2018). Extremism and its modern appearances. – Uzbekistan: The Light of Islam. – 24.

Alexander, L. M. (2019). Terrorism: Theory and practice. – NY: Routledge. – 296.

Denning, E. D (2000). Cyberterrorism. 1-10. Available from:
https://calhoun.nps.edu/bitstream/handle/10945/55351/Denning_Dorothy_2000_cyberterrorism.pdf?sequence=1&isAllowed=y

Onwudiwe, I. D. (2018). The globalization of terrorism. Routledge. – 190.

Osman, K., Alarood, A., Jano, Z., Ahmad, R., Manaf, A. A., & Mahmoud, M. (2019) A Conceptual Model of Cyberterrorists' Rhetorical Structure in Protecting National Critical Infrastructure. In International Conference on Smart Innovation, Ergonomics and Applied Human Factors (pp. 421-427). Springer, Cham.

Rahimjonov, D. (2019) The importance of social rehabilitation of people who have fallen under the influence of extremist ideas in the process of globalization. – Uzbekistan: The Light of Islam. – 12.

Seed, D. (2019) EMP and Cyberterrorism. In US Narratives of Nuclear Terrorism Since 9/11. – London: Palgrave Macmillan. – 233-270.

Topal, R. (2019) A cyber-psychological and behavioral approach to online radicalization. In Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications. IGI Global. – 1031-1042.

Umarov, B. (2018) psychological problems of prevention of extremism and terrorism among young people. The Light of Islam, 2018 (1). – 23.

Vacca, J. R. (Ed.) (2019) Online Terrorist Propaganda, Recruitment, and Radicalization. – Boca Raton: CRC Press. – 532.

Weimann, G. (2004) Cyberterrorism. How real is the threat? December 2004. www.usip.org/

Weimann, G. (2004a) How modern terrorism uses the internet. March 2004. Special report. https://www.usip.org/sites/default/files/sr116.pdf

Zhaholatga qarshi ma'rifat (2019) [Enlightenment against ignorance]– Toshkent: "O'zbekiston halqaro islom akademijasi" nashrijot-matbaa birlashmasi. – 120 (in Uzbek)