ISSN 2459-1149 SHS journal R

JOURNAL OF SOCIAL AND HUMANITIES SCIENCES RESEARCH

Economicsand Administration, TourismandTourism Management, History, Culture, Religion, Psychology, Sociology, FineArts, Engineering, Architecture, Language, Literature, EducationalSciences, Pedagogy&OtherDisciplines

2018
Vol:5 / Issue:24

pp.1446-1458

ArticleArrivalDate (Makale Geliş Tarihi)	29.06.2018
ThePublishedRel. Date (Makale Yayın Kabul Tarihi)	10.09.2018
ThePublishedDate (Yayınlanma Tarihi)	12.09.2018

CYBERTERRORISM AND COUNTER CYBERTERRORISM POLICY IN THE RUSSIAN FEDERATION

Assistant Professor Dr. Demet Şefika MANGIR

Selcuk University, Department of International Relation, Konya/TURKEY

ORCID: 0000-0002-2542-8551

PhD Candidate Mukhammadjon GANİEV

PhD Candidate in Selcuk University, Department of International Relation, Konya/TURKEY

ORCID: 0000-0002-2497-2037

ÖZET

Terörizm çok eski zamanlardanberi varlığı bilinen, ancak terör eylemlerinin yürütüldüğü araçların zaman içinde değişime uğradığı insanlık dişi bir olgudur. Siber uzayın ortaya çıkışı (bilgi teknolojisindeki gelişmeler) bir yandan fırsatları ve diğer yandan da zayıf noktaları ortaya çıkarmıştır. Bireyler ve terör örgütleri siber uzayda siber uzaya saldırmak ve siber-terörizm olgusu için bu kırılganlıklardan yararlanmıştır. Bu yazının amacı, siberterörizmin ortaya çıkışını ve devletlerin siberterörizmi engellemek için kullandığı önlemleri veya politikaları incelemektir. Araştırma, Rusya Federasyonu'ndaki karşı-siber terörizm önlemlerini ya da stratejilerini incelemeye odaklanmaktadır. Bu yazıda kullanılan metodoloji, mevcut literatürlere dayalı nitel araştırmalardır. Sonuç olarak, siberterörizm tüm dünya için ciddi bir sorun haline gelmiştir. Siber-terörizm tehlikesi, devlet sınırlarının ötesinde olduğu için onunla ortaklaşa mücadele etmek gerekmektedir.

Anahtar Kelimeler: Siberterörizm, Bilgi Toplumu, Rusya Federasyonu, Uluslararası toplum, İşbirliği, Tehdit.

ABSTRACT

Terrorism as a phenomenonhas been in existence perhaps since time immemorial but the means by which terrorist acts have been conducted have changed over time. The emergence of the cyberspace (development in information technology) has created opportunities on one hand and vulnerabilities on the other hand. Individuals and terrorist organisations have capitalised on these vulnerabilities within cyberspace to launch attacks with the cyber realm, thus the emergence of cyberterrorism. The objective of this paper is to investigate the emergence of cyberterrorism and measures or policies that states employ to counter cyberterrorism. The research focuses on examining counter cyberterrorism measures or strategies in the Russian Federation. The methodology used for this paper is that of qualitative research based on the available literatures. The conclusion is that cyberterrorism has become a serious problem for the entire world. The danger of cyberterrorism lies in the fact that it does not know the state borders, therefore it is possible to fight it only jointly, and the counter cyberterrorism policy of the Russian Fedaration in insufficient.

Key words: Cyberterrorism, Information Society, the Russian Federation, International community, Cooperation, Threat.

1. INTRODUCTION

The objective of this paper is to research on cyberterrorism as a socio-political phenomenon and the policy of counteracting it in the Russian Federation. The subject of the study is an analysis of socio-political causes, factors that determine the growing threat of cyberterrorism, the trends and peculiarities of its functioning, and the identification of contradictions that affect the process of developing and implementing a policy of countering cyberterrorism in Russian Federation.

The source and empirical basis of the study was made up of normative and legal documents of different countries and international organizations. The normative and legal acts, namely the laws of the Russian Federation, decrees, resolutions and orders of the President of the Russian Federation and the Government of the Russian Federation, including international conventions and declarations regulating the main directions of the development of the policy of countering cyberterrorism, policy documents, information materials of conferences and thematic round tables, political journalism.

The study of the phenomenon of cyberterrorism is one of the most problematic studies in science. This is due to the multifaceted nature of this socio-political phenomenon, which is difficult to express with a single definition. Questions of cyberterrorism are studied in a number of theoretical and applied sciences, such as: political science, sociology, psychology, economics, law and management, etc. Difficulties in studying the phenomenon of cyberterrorism are associated with the development of the information and communication sphere, which covers and affects almost all aspects of the life activity of the socio-political system. The problem of ensuring the security of computer information and technology, today is one of the most acute challenge for most countries in the world. First of all, this applies to the use of information systems and networks in public administration, military and industrial spheres, and business. The development of an effective policy to counter cyberterrorism is carried out in the following main areas: identification of priority goals and means, identification of possible cyber-terrorist threats, protection of the population, establishment and coordination of the international infrastructure, countering cyberattacks, including the development of special anti-terrorism programs, international law, etc. Ensuring security from cyber-terrorist threat is becoming one of the main priorities of Russia's national security. The state implements a policy of countering cyberterrorism in the framework of implementing the basic principles of building an information society. In the fight against cyberterrorism, priority should be given to the rapid suppression of cyber-terrorist attacks at the stage of their preparation (information analysis, development of laws, state control), and monitoring the state of the information and communication space on a regular basis, delivering the necessary information to the public, preventive work (educational, legal, organizational), etc.

The aim of the paper is to study the priority directions of the state policy to counter this type of terrorism, to develop recommendations for the prevention of acts of cyberterrorism, to improve the strategy to combat this negative phenomenon, taking into account Russian experience. The purpose of the study determined the need to solve the following theoretical and empirical problems:

1. to analyze the concept of “cyberterrorism” and define it as a socio-political phenomenon.
2. to identify the political, social, economic and other reasons for the emergence and activation of cyberterrorism at the present stage, its features and functioning trends.
3. to analyze the Russian experience of countering cyberterrorism and reveal its importance for the development and effective implementation of this type of policy in the Russian Federation.
4. to study the priority directions of the Russian state's activity in the issues of countering cyberterrorism.
5. to assess the effectiveness of the state in this segment of the policy, develop recommendations on improving the state policy to counteract this phenomenon.

One can proceed from the scientific assumption that such a relatively new kind of terrorism, like cyberterrorism, in the 21st century has a tendency to spread. Its threat substantially increases due to the widespread development of global networks and the insufficient development of law (legal) and other control mechanisms of the state, as well as during the period of political and socio-economic transformations (Молодчая, 2011, p. 14).However, in stable socio-political systems, the activation of cyber-terrorist activities is possible. Increasing the effectiveness of state policy to counter cyberterrorism will require its comprehensive research, the integration of efforts of state institutions and civil society structures, the early diagnosis of its threats, the development of legal frameworks and setting preventive measures.

2. ANALYSIS OF THE CONCEPT OF CYBERTERRORISM IN THE CONTEXT OF POLITICAL SCIENCE

In the conditions of development of scientific and technical thought, tendencies of universal informatization and computerization arise complex systems for processing data, which include computers, computer networks and systems. Informatization and computerization affect many aspects of state and public life from the issues of ensuring national security to the control of land and air transport. With the wide application of new technologies, it can be noted that the Internet network covers all countries of the world thanks to the use of mobile communication devices. Connection to the Internet is possible from anywhere in the world using satellite and navigation gadgets.

The intensive development of Internet technologies opens new opportunities for developing a coherent policy to overcome political, social and economic crises, as well as to develop measures to prevent them. Despite this, the Internet in its current state is able to act as a potential source of various crisis situations, and can also strengthen them. The information and communication infrastructure of the state is a strategic resource that requires constant monitoring and attention. Any actions of destructive nature in the information environment can have serious consequences for managed networks and systems. According to modern researchers, information networks act as a means of information struggle among politicians, religious organizations, businessmen, various criminal groups and terrorist groups.The social and political consequences of scientific and technological progress often contradict the interests of Internet users who are exposed to various kinds of cyberattacks, especially cyberterrorist attacks. (Хлопьев, 2014, p. 45).

The role and the significance of the study of problems of cyberterrorism and the scientific validity of measures for their resolving sharply increase in the context of the growing complexity of the social structure and political life of the society, the decline in confidence in political institutions and the ineffectiveness of certain mechanisms of influence on societies. This can lead to instability of the organization and functioning of the political system and to the search for new ways of solving existing problems. These and other circumstances dictate the need to develop an adequate effective state policy to counter cyberterrorism. The analysis of cyberterrorism is an actual research and practical task. The theoretical inadequacy of the problem has a negative impact on the solution of practical problems in securing state’s socio-political stability. (Андреева, 2013, p. 134).

The study of the phenomenon of cyberterrorism as a scientific direction has a number of features. First, it has interdisciplinary character, being the subject of research of political, law and technical sciences. Secondly, it has an applied orientation, because is closely connected with the solution of information security problems. All this predetermines the variety of theoretical approaches used to study this phenomenon. (Коломыцев, 2011, p. 47). In order to define this phenomenon, it is necessary to turn to existing scientific approaches, on the basis of which it will be possible to define cyberterrorism in the political aspect.

The term of cyberterrorism, was first used in the 1980s by Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California**.** Collindefined cyberterrorism as “the convergence of cyberspace and terrorism” (Ogren, 1999, p.5). However, in the early 90's, the first cyber attacks were recorded. (Услинский, 2015).To gain a better understanding of cyberterrorism, however, its component terms must be clearly defined:

1. The term of cyberspace was first popularized in a novel named “Neuromancer” which was written by William Gison in 1984. Cyberspace was described by Winn Schwartau as following:

Cyberspace is that intangible place between computers where information momentarily exists on its route from one end of the global network to the other. Cyberspace is the ethereal reality, an infinity of electrons speeding down copper or glass fibers at the speed of light from one point to another. Cyberspace includes the air waves vibrating with cellular, microwave, and satellite communications. (Ogren, 1999, p.5).

One has to know that cyberspace does not only relate to the world of computers, but it's also connected to the entire interconnected world of networks and telecommunications. The medium is irrelevant; cellular telephones, satellite communication links, undersea, wireless local-area networks, token-ring networks, fiber-optic cables, etc. are all part of communication networks and this mesh of information.

2. Terrorism - James M. Poland, a Professor at California State University in California describes terrorism as following: "Terrorism is the premeditated, deliberate, systematic murder, mayhem, and threatening of the innocent to create fear and intimidation in order to gain a political or tactical advantage, usually to influence an audience". (Best & Nocella, 2004, p. 371).

This definition includes all dimensions of terrorism:

a) Premeditated or systematic act of killing or any other type of harming
b) An act that is delivered against innocent people or non-combatants
c) An act that creates fear and intimidation on people
d) An act that is delivered ın order to gain a political aim.

Finally, cyber terrorism can be defined as:

"Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents."(Pollitt, 1997, p. 285-289).In other words cyber terrorism is terrorising people through computer. That is to say, its a terrorist act that is delivered in cyberspace.

The importance of countering cyberterrorism is that the ever-growing interconnection of information and computer systems, which form the core of the state's infrastructure and connection to the internet, is the goal of cyberterrorist acts. This applies primarily to nuclear reactors, air and rail transport management systems, large storage of strategic raw materials for the distribution of electricity and water, chemical and biological laboratories. Threats to critical infrastructures are real. Through interconnection and interdependence, state infrastructures can be vulnerable to new ways of attack. The deliberate exploitation of these vulnerabilities can have serious consequences for politics, economics, security and life. Thanks to the anonymity of the absence of national borders and other opportunities provided by the Internet, potentially dangerous cyber attacks can be conceived and prepared without detection. They can invisibly reconnoiter, secretly rehearse, and then be implemented in minutes or even seconds, without identifying the attacker or establishing his location. Cyber-terrorists use the Internet for the reason that it provides the maximum organizational and offensive capabilities.. Terrorists can organize a major attack by combining traditional terrorist activities with information attacks, with access to modern information technologies that will lead to huge economic losses. (Коломыцев, 2011, p. 87).

Its very clear that the computer is the most likely weapon of cyberterrorists. (Gordon, 2003, p 9) Hackers can get into a system: through Virus, E-Mail wireless networks can be one of the biggest threats to the public because in this case you don't have to be connected to a computer to acquire its information. Cyberterrorism involves crimes of terrorism that occur electronically. Here we can bring some examples of cyberterrorist acts and cyberattacks in general:

On January 25, 2003 in the Republic of South Korea, as a result of the actions of hackers, there was a nationwide Internet failure, within a few hours the entire country was deprived of access to the world network. For the first time, the actions of "cyber-terrorists" affected the activities of companies on a national scale. The main victims of the attack were companies, leading the Internet trade - a failure affected about 17 million of their users who could not access their accounts in online stores. (ИТАР-ТАСС, 2016).

In late April and early May 2007, the websites of Estonian state organizations were subjected to a cyber attack, which caused an international scandal. Access to the websites of the President of Estonia, the Parliament of the country and the Estonian Foreign Ministry, banks and companies was blocked for three weeks. (William, 2009, p.4-8).

In September 2010, the Stuxnet virus hit the computers of employees of the nuclear power plant in Bushehr (Iran) and created problems in the functioning of centrifuges of the uranium enrichment complex in Natanz. According to experts, Stuxnet was the first virus to be used as a cyber weapon. In total, according to the director of the Information Technology Council of the Ministry of Industry of Iran Mahmoud Liai, about 30,000 computers were attacked (Hossein, 2013, p. 132).

January 7, 2015 as a result of the attack of a group of Ukrainian hackers “CyberBerkut”,the websites of the German parliament and Chancellor Angela Merkel did not work for several hours. (Однако SU, 2015).

In February 2016, as a result of hacking, there was a theft of funds of about $ 81 million from the central bank of Bangladesh. (ИТАР-ТАСС, 2016).

According to some researchers, cyber-terrorist attacks are almost impossible to predict or track in real time. Therefore, an attack can begin at any time, at home or abroad, and hostile countries, criminals, spies and terrorists can stand behind it. It will take considerable resources to determine with a high degree of certainty who is responsible for this. Modern technologies in the near future will not be able to solve this problem. (Хлопьев, 2014, p. 107).

The danger of cyberterrorism is that it knows no state borders, in other words it has cross-border nature. Therefore, it is possible to fight it only together, using the resources of the entire world community. This requires coordination of efforts of governments and special services of many states. It should be borne in mind that terrorists are constantly improving the arsenal of means and methods of their activities. Organizations can never be 100% safe from cyberattacks but they can take some precautions. Defense methods include Encryptions, Firewall, Browser Privacy Settimg, Pop Up Blocker, Account Control, Backup System Intrusion Detection System and Changing Passwords regularly. The Law also need to be more effective against someone caught performing cyber terrorism.

3. RUSSIAN COUNTER CYBERTERRORISM POLICY

One of the new and dangerous threats to mankind in the 21st century is the use of information technologies by the terrorist organizations and the global Internet network. Rapid technological advancement in the information age made it difficult to fight crime and opened up new opportunities for global criminal activity. The increased interconnection of our most important infrastructures through computer and information systems has created new vulnerabilities, because criminals, terrorists and foreign intelligence agencies are exploring ways to use the power of cybernetic tools and weapons. The state policy of confrontation with cyberterrorism in the Russian Federation is the activity of the system of federal bodies of state power to counter cyber-terrorist attacks on critical objects of information and communication infrastructure that can lead not only to severe socio-political and economic consequences, but also to great human losses. (Петров, 2009, p. 26).

The policy of countering cyberterrorism in the Russian Federation is based on the principles of legality, the balance of interests of the individual in society, informing the public about the activities of public authorities in this area and priority of national interests. The functions of implementing the policy of countering cyberterrorism are distributed among the following federal bodies: the FSB (Internal Security Service the successor to the KGB, as it was disbanded into the FSB and the SVR in 1991), the SVR (Foreign Intelligence Service the successor to the KGB too), the Ministry of Internal Affairs, the Ministry of Foreign Affairs and the Ministry of Communications and Mass Media. (Алексенко, 2009, p. 99).

The state in the performance of its functions to ensure the security of the Russian Federation in the conditions of a cyberterrorist threat carries out the following tasks:

1. Legal support of the policy of counteraction to cyberterrorism which develops norms of the federal legislation giving a legal classification to cyber-terrorist actions, participates in the development of international law on countering cyberterrorism, develops mechanisms for investigating and prosecuting cyber-terrorist facts, as well as the procedure for eliminating the consequences of cyber-terrorists and

develops normative legal acts taking into account the specifics of the legislation of the Russian Federation.

2. Implementation of the main provisions of the Doctrine of Security, the National Security Strategy and the Concept of Counteracting Terrorism that organizes and conducts comprehensive analysis and forecasting of threats of cyberterrorism in conditions of use by foreign states and terrorist organizations of dangerous aggressive forms of external influence (cyberwar), develops measures and mechanisms for ensuring security in the face of cyber-terrorist threats, organizes the work of legislative and executive bodies of state power to implement a set of measures aimed at preventing, parrying and neutralizing cyber-terrorist threats, monitors the activities of federal bodies of state power to implement the policy of countering cyberterrorism and supports the activities of public associations in the field of countering cyber-terrorist threats.

3. Creation of the state counter cyberterrorism system which develops an official concept of confrontation with cyberterrorism, forms a nation-wide system of confrontation with cyberterrorism, organizes activities to counteract the shares of cyber-terrorist aggression, organizes the activities of the state system of government authorities to quickly respond to identified cyber-terrorist threats, provides representation of the interests of the Russian Federation in relevant international organizations and participates in the creation of systems and the mechanism of collective (international) cybersecurity. (Молодчая, 2011, p. 109-111).

Cybertercrimes have their own specific features of committing and the highest rates of growth and change. In Russian Federation, the number of crimes committed in cyberspace continues to grow steadily. According to the Ministry of Internal Affairs of the Russian Federation about 6000 crimes in the sphere of high technologies were revealed in 2009. In 2010 the number of such crimes increased about 8000. The number of cybercrimes in 2011 increased by 95% as compared to 2010. In 2012, the total number of crimes in the information sphere increased by more than 22% compared to 2011. Since 2012 until now, the number of illegal encroachments in the sphere of computer information has almost doubled and the number of cases of illegal receipt and disclosure of information constituting commercial or banking secrets committed using computer equipment has tripled. (Леонид, 2017, p. 12-14).More serious threats of cyberattacks to the Russian government and banks were confirmed in last several years. For example:

On June 2015, the hacking group “Anonymous International” hacked the e-mail of Dmitry Medvedev's press secretary Natalia Timakova. As a result of the hacking, letters, reports and 500 messages from the personal correspondence of Prime Minister Dmitry Medvedev were put up for sale. This hacking brought a discussion about the need of taking the internet under the control of the authorities in Russian Federation. (Ведомости, 2015).

On November 2016, Sberbank, Alfa-Bank and Otkrytiy Bank were cyberattacked. Difficulties in accessing the organization's website were also confirmed. The chairman of Sberbank, Stanislav Kuznetsov estimates 600-650 billion rubles as annual losses of the Russian economy from cybercrime (Александр, 2017).

On June 2017 virus Petya A hit computers of more than 80 companies in Russia and Ukraine. The virus blocks all files on the infected computers, unlocking the program requires paying $ 300 in the crypto currency of bitcoin. Among the affected companies are Bashneft, Rosnef, Oschadbank, Mars, Novaya Pochta and others. (Ведомости, 2017).

Experts believe that only 5% of cybercriminals become known. The reasons for the high latency of such crimes are different. It should be noted that Russian legislation lags far behind developed countries in the field of criminal and legal protection of computer information. At the same time, the legislation of the Russian Federation has clearly insufficient legal regulation of the responsibility for such crimes, as well as the insufficient knowledge of law enforcement officers in this sphere and their extremely slow adaptation to the new conditions for combating cybercrimes. It should be mentioned that, there is no shortage of qualified specialists capable of solving any technically complex problem in Russian

Federation. However, the low standard of living and the professional lack of demand of high-class engineers lead them to take criminal path.(Королёва, 2014, p. 94).

Cyberterrorism as a multi-aspect socio-political phenomenon of modernity should be countered by a comprehensive system of counterterrorism measures, which will be formed on the basis of building strategic planning and building an effective organization. The solution of the tasks is possible within the framework of the National Security Strategy of the Russian Federation which will be implemented until 2020.This strategy provides for a more narrow range of actions and includes:

the development of the concept of antiterrorist struggle in modern conditions.

– interaction of all law enforcement forces and special services in the antiterrorist struggle, with the allocation of the main body with the necessary powers and rights to organize, coordinate and implement the entire fight against cyberterrorism, and placing responsibility on it for its effectiveness.
– creation of a unified information system, both in Russia and within the framework of the Commonwealth of Independent Stateson combating cyberterrorism and carrying out analytical work to ensure the fight against cyberterrorism.
– development of effective methods of interaction with foreign bodies engaged in combating criminal and political extremism.
– toughening of legal consequences (punishments, sanctions for persons connected with terrorist activities and conducting cyber-terrorist acts, etc.).(КонсультантПлюс, 2009).

The Russian state also implements the policy of countering cyberterrorism in the framework of implementing the basic principles of building an information society. One of the main steps in this direction is a significant improvement in the efficiency of state management. The most effective solution to this problem is the use of nationwide information technology infrastructure called “Electronic State” on the basis of the national space of electronic identification elements, which also allows for high cybersecurity. (Матюхин, 2008, p. 36-42).

By the presidential decree of January 15, 2013, the Russian Federal Security Service (FSB) was authorized to create a state system for detecting, preventing and eliminating computer attacks on information resources of the Russian Federation, information systems and information and telecommunications networks located in the territory of the Russian Federation and in diplomatic missions and consular offices of the Russian Federation abroad. In turn, the US President signed on February 13, 2013, a directive on cybersecurity, which calls for the creation of a country's cybersecurity system and the development of standards and techniques that will help reduce the risks from cyberattacks to the most important infrastructure. (ОружиеРоссии, 2013).

When considering the Russian policy of countering cyberterrism, it is necessary to stop at the international aspect of its implementation:

In 1996 leaders of G8 (Great Britain, Germany, Italy, Canada, Russia, USA, France, Japan) adopted a package of measures in Lyon city which aimed at combating international crime. The package contains specific recommendations on identifying and preventing crimes and terrorist acts committed using advanced technologies. Eight countries will develop common approaches to combating high-tech crimes and computer piracy, including those of terrorists using the latest advances in information technology for penetration into databases of financial institutions and state institutions.(Завер, 2006,p.228).

In December 1998 by the initiative of the Russian Federation, the UN General Assembly adopted a resolution on cybercrime, cyberterrorism and cyberwar. Resolution 53/70 calls upon Member States to inform the Secretary-General of their views and assessments on:

a) problems of information security,
b) definitions of basic concepts related to information security and
c) the development of international principles that improve the global information space and telecommunications, and help combat information terrorism and crime. (Gabriel, 2000, p. 2).

On December 8, 2003, the UN General Assembly adopted a resolution initiated by the Russian side translating the general political discussion of international information security issues into the search for practical solutions. This resolution was supposed to launch the mechanism of the work of the group of governmental experts of the United Nations, however, because of the obstructionist position of the United States, these efforts proved inconclusive. During the reign of George W. Bush, the American delegation twice voted against the adoption of the resolution, effectively opposing the US position to the opinion of the world community. As a result, the work of the group of government experts was paralyzed. (Алексеева,идр, 2004, p. 186-87).

On November 2006 in St. Petersburg during the Global Forum on the Partnership of the State and Business in Countering Terrorism Russia made a number of long-term initiatives to combat cybercrime, which were highly appreciated by foreign partners, received full support and moved into practical plane. It was about protecting critical infrastructures, countering the illegal use of the Internet to promote racial and religious hatred, recruiting terrorists and financing them. (Интелрос, 2006)

On June 16, 2009, an intergovernmental agreement of the SCO member states on cooperation in the field of ensuring international information security was signed in Yekaterinburg. The uniqueness of this document was that for the first time at the international legal level it documented the existence of specific threats in the field of information security, and also defined the main directions, principles, forms and mechanisms of cooperation in this field. Both within the framework of the SCO and in wide international practice, the agreement that entered into force became the first treaty act covering the entire range of problems of international information security from countering cybercrime and cyberterrorism to disarmament issues. This agreement was ratified by four SCO members (Russia, China, Kazakhstan, Tajikistan), and on June 2011 it entered into force. (Бедрицкий, 2012, p. 122).

On May 2010 a bilateral document was signed by Russia and Brazil on the basis of mutual trust and cooperation on information and communication security. Significant progress has been made in the development and implementation of the latest information and communication technologies and communications. Both sides expressed their concern about the threats in civil and military spheres posed by the use of new technologies. (РаспоряжениеПравительстваРоссийскойФедерации, 2010).

On September 12, 2011 at the 66th session of the GA, the Permanent Representatives of the Russian Federation, China, Tajikistan and Uzbekistan to the United Nations proposed a joint project of “Rules of Conduct in the Field of International Information Security”. This project createdprerequisites for further comprehensive discussion of the problem of international information security at the international level. (Бедрицкий, 2012, p. 124).

On March 6-7, 2012, the Russian Center for Science and Culture in Delhi hosted the Russian-Indian scientific seminar “The Conception of the Convention on International Information Security” devoted to the discussion of the draft convention. The organizers of the scientific event were the Institute for Information Security Problems of the Moscow State University named after MV Lomonosov, the Russian Embassy in India, the Defense Research and Development Organization of the Ministry of Defense of India with the assistance of the Rossotrudnichestvo office. February 7-8, 2012 at the 14th National Information Security Forum in Moscow, this issue was also on the agenda. Non-governmental organizations and business joined the discussion of the document. The Russian side conducts bilateral consultations on this issue with its partners. (Андрей, 2012).

In June 2013 Russia and the United States agreed on the need for cooperation in combating “Threats to Information And Communication Technologies in the Context Of International Security”. Russia and the United States often disagreed on the nature of the problem. Russia focuses on “International Information Security”, while the US considers cybercrime, cyber espionage and cyberterrorism as the main threats in this sphere and therefore prefer the term "cybersecurity" and focus on protecting computer networks and resources. Soon after the signing of this agreement, information was large-scale wiretapping of phones and tracking of Internet-correspondence of citizens and governments, which were carried out by US special services. The source of the information was Edward Snowden, a former employee of a contractor company working with the US National Security Agency (NSA). Soon after the US brought charges against Snowden, the Russian authorities granted him asylum. This development has weakened the interest of Russia and the US in further cooperation in the cyberspace. (Олег,Дидр, 2016, p. 7-10). It should be mentioned that back in 1998, Russia invited the United States to sign a statement at the presidential level on information security issues. However, discussion of the draft statement did not lead to the rapprochement of two countries. (Фёдоров,2006, p. 187).

In May 2015, Chinese President Xi Jinping's visit to Moscow was marked signing of a number of agreements between Russia and China. One of them was agreement in the field of international information security, which already received the name “Cyberpact”. The draft agreement says that the Russian Federation and the PRC will not implement cyberattacks against each other. At the same time, they intend to jointly fight threats in cyberspace. This agreement attracted a lot of attention, because it is regarded as an important and symbolic step of Russia and China to each other in one of the most relevant spheres of international relations. Russia and China have announced their intention to work closely together to jointly respond to threats by enhancing interaction and data exchange among relevant law enforcement agencies on cybercrime and terrorism through the sharing of experiences in cyber security technologies and the creation of communication channels that allow for rapid response to cyber threats in the world.(Alexandra, 2015). This agreement worries USA as American government consider it as a threat to its national interests. Some experts attribute the agreement between Russia and China as Russia's desire to limit US influence and create a united front to combat possible cyber transactions.

3.1. Contradictions in the Implementation of Counter Cyberterrorim Policy

It should be noted that there is a contradiction between the needs of society. On the one hand, the realization of constitutional human rights and freedoms in the field of obtaining information and using it, and on the other hand, the necessity of unconditionally securing the law that protect society and the individual. Based on the analysis of regulatory documents of the Russian Federation, we will determine the main contradictions that affect the nature and tendencies of the development of cyberterrorism:

1. Contradiction between the main participants of the global information society, based on the strengthening of the global information confrontation. The need to expand international cooperation in the field of development and the safe use of information resources, counteract the threat of unleashing confrontation in the information and communication environment, contradicts the active development by several countries of strategies and concepts of information wars that create the means of harmful effect on information and communication spheres of other countries of the world. (Воронович,2012, p. 143).
2. Contradiction between the state policy on the speedy transition to the information society and the development gap and the introduction of advanced information technologies. On the one hand, the state policy is aimed at increasing the efficiency of using the information and communication infrastructure in the interests of social development, improving the infrastructure of the unified information space of the Russian Federation, developing the domestic information services industry and increasing the efficiency of using state information resources, and on the other hand, the adoption by federal and regional authorities of normative and legal acts that infringe upon the constitutional rights and freedoms of citizens, the failure of state authorities to comply with the requirements of federal laws in the information sphere, the unlawful restriction of citizens' access to open information resources. (Михайленко,2004, p. 98).
3. The contradictions generated by the statements between power and the population, first of all, this is manifested in the discrepancy between the political statements of the representatives of power and the policy pursued by the state. On the one hand, public statements by the President of the Russian Federation on increasing the "innovation" of the state, improving the state management system based on the use of modern technologies, increasing the state's openness, strengthening its interaction with civil society institutions and business on issues of innovative development, on the other hand, in practice we are faced with the creation of monopolies in the formation, receipt and dissemination of information, the irrational and excessive restriction of the access of Russian citizens to socially necessary information, as well as the latest information technologies in the world information services, information, telecommunications, and information products.(Молодчая, 2011, p. 75).

4. Contradiction generated by the democratization of social life. The world experience of social development shows that a society of an open democratic type creates more favorable conditions for terrorist activity than, for example, an administrative command system with its rigid, total control both over the behavior of an individual person and, of course, the functioning of all socially political institutions. Democratization of society can contribute to strengthening the influence of these factors on the socio - political life of society. On the one hand, it is necessary to ensure the constitutional right of a person and a citizen to freely seek, receive, transmit, produce and disseminate information, also guarantee the freedom of mass information and prohibit censorship, and on the other hand, not to allow propaganda and agitation that foments social, racial, or religious hatred and enmity. (Карнаушенко, 2014, p. 197).

This group of contradictions through various factors has an impact on stimulating cyberterrorism and weakening the ability of state authorities to effectively confront it.

3.2. Increasing the Effectiveness of Counter Cyberterrorism Policy

Thus, in order to increase the effectiveness of the fight against cyberterrorism in Russian Federation and CIS it is necessary:

1. creation of a unified information system, both in Russia and within the framework of the CIS on combating cyberterrorism.
2. to create a national data bank on cyberterrorism for forecasting and simulating crisis situations and developing optimal response measures (operational actions) for cyberincidents.
3. to accelerate the development and adoption of the Law on Combating Cyberterrorism especially the development of the concept of antiterrorist struggle in modern conditions.
4. to organize scientific and methodological support to develop recommendations and proposals to update the fight against cyberterrorism.
5. to add to the Criminal Code additions in terms of attributing cyberterrorism, toughening of legal consequences (punishments, sanctions for persons connected with terrorist activities and conducting cyber-terrorist acts, etc.).(Молодчая, 2011, p. 131-132).

Such a large-scale task will require a lot of time and significant costs. However, the prevailing reality is that the existence of a country is largely determined by its ability to timely form an effective response to the challenges of the outside world. Therefore, the decision to establish an effective national system to counter cyberterrorism is one of the main priorities of the national security of the Russian Federation.

4. CONCLUSION

In the contemporary world, there is a growing dependence of state authorities, industrial enterprises, public organizations and individual users on information and communication technologies in the performance of their functions, business management, information exchange, and provision of public services. As a result of increasing interconnectedness, information systems and networks are subject to ever-increasing and diverse threats that create new security challenges. Information has become a valuable asset for individuals, businesses, organizations and states. When important data cannot be effectively protected, the personal security of people, business and more importantly the national security of the state remain under threat. The development of information and communication technologies opens new opportunities both for overcoming crises and for developing a coordinated policy to prevent them. However, in its current state, the Internet itself can act as a potential source of crisis situations, and may also strengthen them according to the principle of resonance. The socio-political consequences of technological progress often come in conflict with the humanistic ideals of civilization, as well as with the interests of millions of users suffering from various kinds of acts of cyberterrorism. Today, cyberterrorism has become one of the ways of solvingpolitical, social, economic, national, religious and personal problems of many people, groups and organizations. Acts of cyberterrorism are especially often used by those people and groups who cannot achieve their ideas of reorganizing the world in an open political dialogue or rivalry.

A complex task is the prevention of acts of cyberterrorism, since this phenomenon is engendered by many political, social, economic, historical, psychological and other reasons. Therefore, such reasons should be the object of constant attention and preventive interference by the state and civil society. Timely detection of cyberterrorism threats, effective policy of counteraction, as well as minimizing the consequences of acts of cyberterrorism in the world in its most diverse manifestations is what the civilized society needs to achieve. Effective struggle against cyberterrorism is one of the main elements of ensuring security. In the field of security, the situation is indeed potentially troubling, but, despite this, there are a number of possibilities for resolving them.

a) Organization of international cooperation with foreign states, their security services and law enforcement agencies, as well as with international organizations, whose task is to combat cyberterrorism and transnational computer crime.
b) Development and improvement of a special unit to combat cybercrime and the creation of an international node for providing comprehensive assistance in transnational computer incidents.
c) Expansion of international cooperation in the legal (law) sphere in combating computer crime and cyberterrorism.
d) Adoption of laws on information security that meet the requirements of the Council of Europe Convention on Cybercrime and current international standards.

Cyberterrorism has its own specific features of the environment of committing and the highest rates of growth and change. At the same time, Russian legislation clearly has insufficient legal regulation of responsibility for this type of crime for effective counteraction to it, as well as lack of knowledge of law enforcement officers in this sphere of relations and their extremely slow adaptation to new conditions for combating cyberterrorism. The importance of researching security problems from attacks of cyberterrorism is determined by the fact that the number of such crimes increases every month, and no structure, be it a private enterprise or state bodies, is insured against these encroachments in the future. The desire of all members of the international community to resolve the problem of countering cyberterrorism will largely depend on the effectiveness of the policy pursued.

The solutions to the problem of cyberterrorism are not simple and unambiguous. Cyberterrorists and their actions must be tied to the law. This should be done in the context of both national and international counter cyberterrorism policies. The severity of the terrorist threat can not be ignored by Russia or other countries. The determination to take the necessary measures can be realized within the framework of new effective international laws and with a new view on their effectiveness and applicability. The solution of the problem of combating this dangerous phenomenon is a task that requires the unification of efforts and the good political will of the entire world community. The comprehensive implementation of appropriate measures in Russia will contribute to ensuring international security from cyberterrorist threats, as well as protecting the interests of the state, society, and the individual. The solution of these national tasks are very important both for cardinal improvement of the current policy of countering cyberterrorism and for further planned and sustainable development of the state. It can be summarized that information technology has not only firmly established itself in the current political process but also has a direct impact on it, even sometimes creates new phenomena and forms in the political life of society.

REFERENCES

Alexandra, K. (2015). *China-Russia Cyber-Security Pact: Should The US Be Concerned?*. Russia Direct. http://www.russia-direct.org/analysis/china-russia-cyber-security-pact-should-us-be-concerned[Accessed: 16. 12. 17.].

Best, S., & Nocella, A. J. (2004). *Terrorists or Freedom Fighters?: Reflections on the Liberation of Animals* (1st ed.). New York: Lantern Books.

Gabriel, R. (2000). *Developments in the field of information and telecommunications in the context of international security*. (United Nations Report No. A/55/554). Retrieved from United Nations http://www.un.org/documents/ga/docs/55/a55554.pdf[Accessed: 16. 12. 17.].

Gordon, S. (2003). *Cyberterrorism?.*Cupertino: Symantec.

Ogren, J. G. (1999). *Responding to the threat of cyberterrorism through information assurance*. California: Monterey.

Pollitt, M. M. (1997). "*Cyberterrorism: Fact or Fancy?" Proceedings of the 20th National Information Systems Security Conference*. pp. 285–289.

Hossein, K. (2013). *Cyber Attacks From The Perspective Of İnternational Law*. 20(1), 132.

William, C. (2009). *Impact Of Alleged Russian Cyber Attacks. Baltic Security & Defence Review*. 11(1), 4-8.

Александр, Щ.(2017). *Сбербанк оценил убытки экономики РФ от киберпреступности в 600-650 млрд рублей в год.*http://tass.ru/ekonomika/4766024, [Accessed: 05. 12. 17.].

Алексеева,И., Авчаров,И.,&Бедрицкий, А. (2004).*Информационные вызовы национальной и международной безопасности*(1-е издание.). Москва:ПИР-Центр.

Алексенко, М. (2009). *Национальная Безопасность России*(1-е издание.). Москва: Научный Эксперт.

Андреева, Ф. (2013).*Принципы Информационного Общества*(1-е издание.). Киев: Инфоарт.

Андрей, Н. (2012). *Борьба Вокруг Проекта Конвенции ООН О Международной Информационной Безопасности*. https://www.fondsk.ru/news/2012/07/14/borba-vokrug-proekta-konvencii-oon-o-mezhdunarodnoj-informacionnoj-bezopasnosti-15499.html[Accessed: 14. 12. 17.].

Бедрицкий, А. В. (2012).*Международные Договорённости По Киберпространству: Возможен Ли Консенсус?*. Оборона и Безопасность. № 4.

Ведомости, (2017).*Кибератака не сказалась на работе крупнейших российских банков*. https://www.vedomosti.ru/finance/news/2017/06/27/698967-kiberataka-rossiiskih-bankov[Accessed: 03. 12. 17.].

Ведомости, (2015). *Хакерская атака не повлияла на работу сайта Кремля.*https://www.vedomosti.ru/politics/news/2017/12/25/746488-priostanovlenii-deyatelnosti-mutko [Accessed: 03. 12. 17.].

Воронович, Н. К, (2012).*Интернет как Угроза Информационной БезопасностиРоссии* (КандидатскаяДиссертация, Краснодарский Университет МВД России, Краснодар, Россия).http://www.dissercat.com/content/internet-kak-ugroza-informatsionnoi-bezopasnosti-rossii[Accessed: 01. 12. 17.].

Завер, Г. (2006). *Преступления Международного Характера в Глобализирующемся Мире*(1-е издание.). Москва: Олма-Пресс.

Интелрос, (2006).*Заявление Участников Саммита «Группы Восьми» О Противодействии Терроризму — Безопасность В Эпоху Глобализации.*http://www.intelros.ru/strategy/g8/678-zajavlenie_uchastnikov_sammita_gruppy_vosmi_o_protivodejjstvii_terrorizmu__bezopasnost_v_jepokhu_globalizacii.html[Accessed: 01. 12. 17.].

ИТАР-ТАСС. (2016). *Крупные атаки хакеров в 2001-2016 годах*. http://tass.ru/info/1408961[Accessed: 16. 12. 17.].

Карнаушенко, П. (2014).*Информационная Безопасность И Антитеррористическая Деятельность Современного Государства* (1-е издание.). Москва: Научный Эксперт.

Коломыцев, О (2011).*Информационная Война* (2-е издание.). Москва: Норма.

Консультант Плюс, (2009). Указ Президента РФ от 12.05.2009 N 537 (ред. от 01.07.2014) *О Стратегии национальной безопасности Российской Федерации до 2020 года*.

http://www.consultant.ru/document/cons_doc_LAW_87685/b8395c52554f9f2b560ff36e8ce0f5bd7808dcc0/[Accessed: 13. 12. 17.].

Королёва, А. В. (2014). *Борьба с Киберпреступностью и Кибертерроризмом* (1-е издание.). Москва: Союз

Леонид,Л. (2017).*Усилить щит от Киберагрессии*. Полиция России.№ 8.

Матюхин, В. (2008). *Информационно-технологическая инфраструктура предоставления государственных услуг населению и организациям как неотъемлемая компонента «Электронного Государства»*. Материалы Российского научноэкономического собрания *Проблемы Модернизации Экономики и Экономической Политики России*.Москва:Научный эксперт.

Михайленко, Е. (2004). *Проблемы Информационно-Правового Регулирования Отношений в Глобальной Компьютерной Сети Интернет*. (КандидатскаяДиссертация, Московский Гуманитарный Университет, Москва, Россия).http://www.dissercat.com/content/problemy-informatsionno-pravovogo-regulirovaniya-otnoshenii-v-globalnoi-kompyuternoi-seti-in[Accessed: 28. 12. 17.].

Молодчая, Е. Н, (2011). *Политика Противодействия Кибертерроризму в Современной России: Политологический Аспект* (Кандидатская Диссертация, Российский Государственный Социальный Университет, Москва, Россия).http://www.dissercat.com/content/politika-protivodeistviya-kiberterrorizmu-v-sovremennoi-rossii-politologicheskii-aspekt[Accessed: 06. 12. 17.].

Однако.SU, (2015). *Хакеры Атаковали Сайты Правительства Германии.*http://odnako.su/news/politics/-244419-hakery-atakovali-sayty-pravitelstva-germanii/[Accessed: 17. 12. 17.].

Олег, Д., Виталий, К., Елена, Ч., Томас, Р., &Крис, С. (2016). *К российско-американскому двустороннему сотрудничеству в сфере кибербезопасности.*https://futureofusrussiarelations.files.wordpress.com/2016/06/2016_05_16_wg_working_paper7_ru_final.pdf[Accessed: 16. 12. 17.].

Оружие России,(2013). *Кибертерроризм: угроза национальной и международной безопасности.* http://www.arms-expo.ru/news/archive/kiberterrorizm-ugroza-nacional-noy-i-mezhdunarodnoy-bezopasnosti14-03-2013-18-35-00/[Accessed: 11. 12. 17.].

Петров, Г. Г. (2014). *Кибербезопасность и кибертерроризм*. Москва: Парад.

Распоряжение Правительства Российской Федерации, (2010).*О подписании Соглашения между Правительством Российской Федерациии Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности*. http://sbornik-zakonov.ru/25132.html[Accessed: 17. 12. 17.].

Услинский, Ф.А. (2015) *Кибертерроризм в России: его свойства и особенности*. http://xn----7sbbaj7auwnffhk.xn--p1ai/article/3476[Accessed: 14. 12. 17.].

Фёдоров А. В. (2006)*Информационная Безопасность В Мировом Политическом Процессе.* Москва: МГИМО-Университет.

Хлопьев, И. (2014) *Философия Информационной Войны*. (2-е издание.).Санкт-Петербург: Мир.