The American Journal of Interdisciplinary Innovations and Research (ISSN–2642-7478)
Published: September 09, 2020 | **Pages:** 1-9
Doi: https://doi.org/10.37547/tajiir/Volume02Issue09-01

IMPACT FACTOR 2020: 5. 498

Journal Website: http://usajournalshub.com/index,php/tajiir

Features Of The Fight Against Modern Virtual Terrorism

Nuriymon Abulhasan
Researcher,National University of Uzbekistan named after Mirzo Ulugbek, Uzbekistan

ABSTRACT

This article analyzes cyberattacks, virtual crime and its ideological basis, as well as implementation technologies as a factor that negatively affects the socio-political stability of society. Trends in the use of virtual technologies in the social life of society and in the context of increasing human impact on daily life, the latest indicators in this regard are given. At the same time, the article assesses their impact on the socio-political stability of society based on the analysis of the concepts of cyberterrorism, cyber-attack and cybercrime manifested in the virtual space.

KEYWORDS

Stability, virtual, terrorism, cyber attack, cyberterrorism, virtual terrorism, internet, cybercrime, virtual space.

INTRODUCTION

At present, the problem of ensuring socio-political stability is being discussed in society to an urgent extent, and this circumstance, we can say, determines the political power of each state.

Stability is the main condition for the development of any modern society. It should be emphasized that full development requires stability in all areas of social society. A positive and qualitative change in one area should not cause confusion and crisis in another, only then will it be possible to ensure the country's strategic progress. The word "stability" refers to the absence or ability of the state to eliminate the real threat of illegal violence in society.

The American Journal of Interdisciplinary Innovations and Research (ISSN–2642-7478)
Published: September 09, 2020 | **Pages:** 1-9
Doi: https://doi.org/10.37547/tajiir/Volume02Issue09-01

IMPACT FACTOR 2020: 5. 498

Stability-means the leadership of a single government over time and the ability to effectively adapt to changing events accordingly. But the transition from stability to disorderly behavior is not determined solely by government support. Because the existence of a Constitutional system in democratic States can be considered as a factor determining stability. Only by ensuring the rule of law in the activities of the political leadership can stability be established. Instability arises from a lack of changes in the composition of the political system or a lack of managerial ability.

MAIN PART

Instability arises from the inability of self-government. In this case, the unstable situation in society may increase, which will attract consequences of varying degrees. To disrupt stability, the situation of using modern technology is becoming more and more acute.

For example, today, with the pace of Internet acceleration, it becomes most relevant to find the answer to the question "how should I live today?» How can you make the most of the "global mind" without losing it (the virtual world) yourself? How dangerous is the problem of online extremism in our society? Why do innocent children and young people suffer from it? what should be done? Just 20 years ago, only 4.1% of the world's population was able to use the Internet. And by 2019, the number of global network users exceeded 4.5 billion. This means 58.8% of all humanity. The importance of the Internet in our lives is highlighted by the UN. The adoption of the resolution on the use of the Internet as a fundamental human right and the call of member countries to fight against digital inequality shows the organization's attitude to the Internet and its achievements [11]. The mass spread of the Mydoom email virus called Novarg & Shimgapi on the night of January 27, 2004 was the beginning of a period of computer terrorism in the history of the world Internet. According to experts, due to the spread of the Mydoom epidemic, the supposedly "victorious campaign" of Internet viruses began. In a few hours, a malicious virus spread through e-mail and the KaZaA file sharing network disabled more than 300 thousand computers in 200 countries. The damage caused by this version of Mydoom amounted to several billion dollars. Currently, the damage caused by viruses of various degrees is 30 billion dollars. According to Kaspersky lab virologist Alexander Gostev, some evidence shows that the Mydoom epidemic was spread by a group of criminals who carefully prepared for it in advance. Virtual technologies create real conditions for a person to earn money, but this process is not always carried out legally. For example, combining groups of cybercriminals helps to increase revenue from their activities. But their actions lead not only to socio-economic, but also to political problems. Viral epidemics will never end. Because these epidemics are the first signs of a new form of cybercrime. Financial and political motivations on the part of some individuals are the reason for their further development. Virologists complain that in our century there are many people who have no idea about antivirus protection. According to the latest research by Panda Software, more than 66% of users from the European Union do not have sufficient antivirus protection or have not installed any antivirus programs at all or have not updated them in a timely manner[15]. In the future, the range of influence of terrorism will be measured by the degree of virtual threats. While such politically motivated threats have not yet led to widespread disasters, they may cause serious tragedies in the future. Several

years ago, during the discussion between China and the United States of the incident with the spy plane of America and the United States, hackers were organized to attack 1,200 websites of the White house, the Department of Energy and the Air force. As a result of this attack, some sites were disabled, and some were completely destroyed. Exactly the same attack was carried out by hackers in Russia and Eastern Europe during the war in Kosovo, and the Pakistanis and Indians are still waging such actions against each other. According to US experts, Russian hackers have been hacking the Pentagon's computer networks for several years and illegally downloading large – scale military-technical information [14].

Cyber attacks can cause various problems in water and electricity supply systems, oil and gas plants and storage facilities, electronic banking networks, telecommunications, transport and emergency services. Terrorists can stop the operation of these systems, or even worse, they can completely disable them, which will lead to various disasters. For this reason, most government agencies and most commercial firms have disconnected their most secret elements of the computer system from the Internet. But it is very difficult to protect these systems from workers. Accidentally mentioned in the press, and immediately removed from the air, a similar case occurred in 2000 in Russia. At the beginning of the year, a Gazprom employee spent several hours helping a group of hackers log into a computer system and a gas distribution scheme for pipes[14].

It became known that the Imam of the mosque located on the square Finsler North London, Abu Hamza al - Masri gathered about himself a group of professionals who are able to hack into a computer system. This proves that Islamic extremists are aware of the potential of computer terrorism. Another Russian expert on computer crimes says that it is not for nothing that American experts are interested in the hacker club of Pakistan, which are supporters of Pakistan in the war against India. The search for programmers to carry out cyber attacks, both by al-Qaeda and other criminal organizations, also has its own interests and is carried out for a reason. Because they have money and they are looking for intelligence. Sooner or later, experts will find it. That is why timely confrontation against such threats should become the most important strategic task of each state. Modern society is becoming more and more involved in the information residence, and the more people's daily lives are intertwined with new advances in digital technology, the more types of terrorist movements they face. As a result of the intrusion of globalization and digital technology into everyday life, a new social residence called virtual truth has emerged. In modern science, virtualization refers to an identity called a cyber-surface. Therefore, the widespread use of information technology in society creates new problems and threats. If until recently the Internet was widely used by scammers for the purpose of financial enrichment, now the possibilities of the virtual world have passed into the hands of even more dangerous players who pursue mainly political goals. In terms of its scale, technical capabilities and consequences, modern cyberterrorism, along with traditional terrorism and organized crime, can pose a serious threat to the life of humanity.

Before continuing the analysis of this new problem of modern society, it is necessary to determine the meaning of some of the terms used. What is cyberterrorism? Based on the initial stages of studying the problem, we do

not have a common opinion on what threat cyberterrorism is considered by the social Sciences.

The term "Cyberterrorism" was applied in 1980 by Barry Collin, a senior fellow at the California Institute of security and intelligence. At that time, the ARPANET division of the us Department of Defense, which Is the defense of the Internet, combined several computers in the same state. However, the expert stressed that soon the capabilities of the Cybernet will be considered by terrorists. In 1997, FBI agent mark Pollitt proposed to consider cyberterrorism as "an attack with a deliberate political bias, without military goals, aimed at damaging information, computer systems, programs, and information that will lead to violence against a group of people or secret agents" and developed a new legal term [6].

Since “cyber terrorism” has similarities with information warfare and the process of using information weapons, the definition of the term “cyber terrorism” will cause, on the one hand, some difficulties for scientists in the process of defining the problem associated with its use. It is usually not difficult to distinguish it from digital crime and digital crime. On the other hand, there is a growing need for new research directions to study and define the characteristics of this form of terrorism. Thus, the economic and psychological signs of cyber terrorism are closely interconnected, so it is very difficult to determine which one is more important. Such scientists as J. Devost, B.Kh. Houghton, N.A. Pollard evaluate digital systems, networks and their constituent parts as a specially designed system of cyber terrorists for the purpose of carrying out terrorist operations or actions [8]. However, most experts say that the term "information crime" means hacking the system, stealing or destroying information for personal reasons, or the actions of a group of hooligans trying to use the information to their advantage. All of them, as a rule, can be said to be one-time crimes against a certain object of a cyber attack. Various types of crimes such as illegal intrusion into computers, computer programs, computer systems, or changing computer data without permission are used in cyber attacks. The main distinguishing feature of cybercrime is characterized by the mercenary assumptions of the attacker. Cyberterrorism differs from the above-mentioned crimes primarily by the goal that is pursued in ordinary political terrorism. When carrying out this attack, the information means of carrying out terrorist actions may be different and may include all types of modern information weapons. At the same time, the tactics and methods of its application differ significantly from the methods of information warfare and information crime. Cyberterrorism is very different from a hacker or computer thief who acts for the purpose of self-enrichment or hooliganism. The main task of virtual terrorism is not only to ensure that the committed terrorist act leads to dangerous consequences and becomes widely known to the population, but also to ensure its acceptance by the General public[8]. As a rule, the conditions of cyberterrorists are characterized by the fact that they do not specify a direct specific object that is subject to an information attack, in order to continue to create a risk of repetition of actions.

In modern social and humanitarian science, there is not even an exact definition of cyberterrorism. In criminal practice, cyberterrorism is not committed in its true form. in most cases, it is observed together with other types of terrorism, including biological, chemical, transport, etc. Some

scientists understand cyberterrorism as a set of actions aimed at attempting to kill a person in order to achieve superiority in solving economic or social problems, destructive actions, distortion of objective information, or other actions that cause fear and aggression among the public. Others see it as a deliberate attack on information processed by a computer, computer system, or network. If such actions are committed for the purpose of violating public security, intimidating the population, or inciting military disputes, they create a serious danger to the life and health of people [7].

The concept of information terrorism should be distinguished from the concept of using information for the purpose of terrorism. Within the framework of journalistic literary publications, these concepts are mostly confused and when it comes to the implementation of information terrorism, it is considered as propaganda work for the purpose of committing terror[13]. When it comes to modern cyberterrorism, it should be understood that this is a multi-faceted phenomenon that encroaches on the lives and health of people, manifests itself in a well-founded political attack that carries threats to the virtual world or causes other serious consequences. In most cases, cyberterrorism manifests itself in a mutual relationship with actions aimed at disrupting public order, creating a threat to the security of society, intimidating the population and disrupting the infrastructure of cities.

A peculiar feature of cyberterrorism is to exert a direct influence on society by intimidating people, weakening the willpower of members of society, and dispelling feelings of panic and distrust among the population. This can be achieved by spreading information about various types of threats, keeping people in constant fear in order to achieve political and other interests, forcing people to take certain actions, as well as by attracting the attention of a terrorist organization to itself. The main goal of a terrorist cyberattack is not only to demonstrate their technical abilities and capabilities (this hooliganism is characteristic of hackers), but also mainly to influence the political power of the state with their help. Professor of information science at Georgetown University USADen assesses cyberterrorism as "an illegal attack or threat to computers, networks and data in them, forcing the authorities to provide assistance to achieve political or social goals"[10]. Comparing cyberterrorism with other types of virtual crimes, it can be argued that cyberterrorists use the same technical means as information terrorists, but their goals differ in socio-economic and political content. Cyberterrorism has a universal character in terms of its impact on society, because it affects all spheres of society, which distinguishes it from other types of crimes. Due to the almost one hundred percent integration of society in developed countries with digital technology, the virtual world plays a large role in human life, sometimes even more than real events. The problem of cyber-terrorism becoming a global phenomenon. This shows that ensuring the security of information has become an important factor in ensuring state sovereignty and national security. Today, the degree of virtual threats is growing all over the world. The number of threats is growing and the consequences of various cyber attacks now have not only a regional degree, but also in their essence and scale reach a global degree. For example, the spread of the "WannaCry" virus in may-June 2017 caused great damage to information sources in 150 countries, including Russia [5].

The American Journal of Interdisciplinary Innovations and Research (ISSN–2642-7478)
Published: September 09, 2020 | **Pages:** 1-9
Doi: https://doi.org/10.37547/tajiir/Volume02Issue09-01
IMPACT FACTOR 2020: 5. 498

The threat of cyberterrorism is very large and in some cases it is impossible to prevent it. In today's society, we need to develop an effective system to combat virtual threats. This requires a comprehensive analysis. In this process, it is advisable to consider the weakest points that can become targets of attack or attack by cyberterrorists. It should be noted that the influence of the information society is also growing dramatically in our country. The ability to conduct external Internet channels at the end of 2018 increased 10 times and today reaches 1200 Gbit/s. To date, this is enough to meet the needs of all providers and operators in Uzbekistan. During 2019, for operators and providers connected to the International packet switching center, the tariff prices for connecting to external channels were lowered from 85 thousand soums to 70 thousand soums (by 17%) per 1 Mbit/s. All this shows a reduction in Internet service rates in Uzbekistan by an average of 4 times, in particular, an increase in Internet speed for all users of Uzbekistan by almost 2 times. According to the company, web services Speedtest.net the company Speedtest Global Index, which collects data on the speed of mobile and wired Internet around the world, noted that the Internet speed in Uzbekistan for the month of November 2019 increased by 11 steps on the rating ladder. Our country ranked 108th among 180 countries in the world (11 steps higher). This is the most reliable increase in a year! The Internet speed in Uzbekistan recorded in November 2019 was 21.47 Mbit/s, while in November 2018 it was 9.98 Mbit / s, which means a 2-fold increase in speed [12].

The main goal of modern terrorism is to create protests among the population and weaken the state by using the terrorist threat of various degrees. From a practical point of view, people who are inclined to protest can, through the implementation of two political strategies, cause a mass protest in society. First, they use economic means, including direct use of paid services, they are withdrawn from persons who have joined the ranks of radical societies, and terrorists always plunder conquered territories, in addition, they try to get money by seizing[2]. To increase the loyalty of their supporters, terrorists help them in matters of food, shelter, and security. For example, one of the peculiar features of the Taliban in Afghanistan is that they allegedly protect citizens from disenfranchisement and violence[1]. The second strategy that can be observed by supporters of terrorists is the punishment for not participating in a political protest. Terrorist leaders cause serious harm to individuals and citizens who do not participate in violence and who prefer to support the legitimate government[4].

The Internet audience of Russians is one of the largest in Europe.it consists of 80 million users, 72 million of them (61% of the population) use online mode every day. This is a very large number and it is growing every day. This number is mainly growing due to young people using the Internet via smartphones. According to information received from the Russian branch of the research concern GfK Group, the number of citizens aged 16-29 years who visit the Internet today is 97%. Thus, the youth layer (97%) is an active Internet user, it is convenient for them to communicate, share photos, watch videos, get acquainted with information, listen to music via smartphones [3].

To the question: "Have you expressed your opinion or your attitude to events or cases on social networks?", the young people replied: "Yes, on their own page." However, as it turned out, the more social networks occupy a

place in the lives of young people, the more criticism they are subjected to. The reason is clear: recently there have been too many social networks, and naturally the number of "calls" related to the health and worldview of young people has increased. I.e., calls to suicide, calls to join a radical religious organization, calls to participate in an unauthorized rally, slanging in comments, Frank communication on forbidden topics, creating pornographic snap chats, etc.the possibilities of social networks have a bad impact on the behavior of young people. The worst thing is that it will not be easy to take away the habits of young people. The Internet has become an integral part of the life of information-hungry, active and creative young people. From this point of view, representatives of parent organizations began to enter the agenda of parse issues in large meetings and control the virtual world, while debates, discussions, development of cases, further no promotion.

Recently, at the Kazan creative industry residence, the question was raised: "Do I need to" treat " young people from the Internet?» Well-known blogger Niyaz Latipov and candidate of psychological Sciences psychotherapist Ramil Garifullin spoke. The first of them believes that you can not allow Internet restrictions, he compared it to restrictions on swimming. Ie, if someone drowned, then "the water is not to blame"! According to Latipov, you need to teach those who stand on the shore to swim - you need to learn how to live on the Internet. Then it will serve as a habitat where you can make friends and develop your intelligence. And psychotherapist Ramil Garifullin denied it. In his opinion, young people need to be "treated"! Not personally from the Internet, but from its psychoneurological consequences: alienation, voluntary loneliness, excessive self – esteem-hypertrophy, unprecedented, antisocial movements. Just as alcohol addiction is not noticeable to the sufferer, so addiction to "likes" is a serious disease. The reason for the increase in the number of suicides in youth groups in social networks should also be found here. This means that we need to establish serious control over the use of the Internet [3].

CONCLUSION

This means that modern virtual terrorism manifests itself in the following areas: first, causing material and economic damage by invading the security system, stopping activities or completely blocking communication systems, public transport, and military facilities; second, exerting psychological influence on large segments of the population in order to create instability and disrupt order; third, exerting psychophysiological influence on individual social groups or individuals involved in the information sphere; fourth, spreading false provocative information that causes military, international, and religious clashes and disrupts the stability of forces in the international arena; fifth, propaganda of radical and extremist ideas, attracting new members to the ranks of existing terrorist organizations; sixth, false warning of the country's human rights bodies about an explosive device installed on their territory, preparation of a terrorist act, etc.; seventh, exerting pressure on the government to make a decision by intimidating a terrorist act; as well as forms of virtual threat are the threat of spreading secret information about the state information infrastructure, intimidation by disclosure of social information, intimidation by disclosure of secrets of the military information system, disclosure of encryption

codes, intimidation by disclosure of the principles of the encryption system, experience in ensuring information security.

REFERENCES

1. Eck, K. Coordination in Rebel Recruitment / / Security Studies 2014. Vol. 23, N 2. P. 364-398, DoI: 10.1080/09636412.2014.905368.
2. Gates, S. Recruitment and Allegiance: the Micro-foundations of Rebellion / / Journal of Conflict Resolution, 2002. Vol. 46, N 1, p. 111-130.
3. Muhammadsidiqov, M.(2018). The influence of "religious factor" on ethno-political and confessional conflicts in Muslim countries. The Light of Islam. Vol. 2018: Iss. 1. Available at: https://uzjournals.edu.uz/iiau/vol2018/iss1/18
4. Азимов, Хабибулло Якубович .(2020). Кашмир муаммоси: тарих ва бугун. ҚарДУ Хабарлари. 1 (1), 180-185
5. Real threats to the virtual world // http://elitat.ru/opinion/realnye-ugrozy-virtualnogo-mira/. - 18.09.2017
6. Азимов, Хабибулло Якубович.(2020). Сурия инқирози даврида Туркия-Россия муносабатлар. Imom Buxoriy saboqlari 1 (2), 86-88
7. Iannacone L. R., Berman E. Religious Extremism: The Good, the Bad, and the Deadly / / Public Choice. 2006. Vol. 128, N 1, p. 109-129.
8. Azimov H.Y. (2019) The emergence of the Syrian crisis and the impact of the external forces on it. Bulletin Social-Economic and Humanitarian Research. № 4 (6). Pp. 92-97. (In Engl)
9. Vladimir Putin discussed measures to combat cyber threats with members of the Russian security Council // News. The first channel. //URL: https://www.1tv.ru/news/2017-10-26/335153\vladimir_putin_obsudil_s_chlenami_soveta_bezopasnosti_rossii_mery_borby_s_kiberugrozami (date accessed: 23.02.2018).
10. Kapitonova E. A. Features of cyberterrorism as a new type of terrorist act // Social science. Right. 2015. no. 2. Pp. 29-34.
11. Kapitonova E. A. Features of cyberterrorism as a new type of terrorist act // Social science. Right. 2015. no. 2. P. 5.
12. Thomas T. L. Deterrence of asymmetric terrorist threats facing society in the information age / / World community against the globalization of crime and terrorism. Proceedings of the international conference, Moscow, 2002.
13. Ravshanov, Fazliddin Ravshanovich, Rashidov, Feruz Tuigunovich, & Azimov, Habibullahan Yakubovich (2020). Amir Temur and Turan States. Bulletin Social-Economic and Humanitarian Research, (5 (7), Pp. 70-81.
14. Turonok S. G. Information terrorism: development of a counteraction strategy / / Social Sciences and modernity. 2011. no. 4. Pp. 131-140.
15. Turonok S. G. Modern terrorism: essence, causes, models and mechanisms of counteraction. Moscow, 2008.
16. Muhammadsidikov, M. (2009) Religious tolerance as the main feature of the public life of Uzbekistan. Eurasian Journal of

Regional and Political Studies, (40), Pp. 69-72. (In Uzbek)

17. is the Internet more expensive in Uzbekistan than in other countries? //http://xs.uz/uzkr/post/ozbekistonda-internet-boshqa-davlatlarga-nisbatan-qimmatmi. - December 16, 2019
18. The Development Of The Internet In Uzbekistan . Results of the year and plans for 2020god//https://pv.uz/uz/news/razvitie-interneta-v-uzbekistane-itogi-goda-i-plany-na-2020-god
19. Farvazova Yu. R. Improving information security as part of Russia's anti-terrorist strategy // Bulletin of the Kazan law Institute of the Ministry of internal Affairs of Russia. 2014. no. 1. Pp. 116-120.
20. Muhammadsidiqov, M. (2015) Stability of North African Region. Int. J. of Multidisciplinary and Current research, 3. (In Eng)
21. Azimov, H. (2019) The problem of Moro Muslims. ISJ Theoretical & Applied Science 6 (74), 519-521
22. Каримов, Н. Р. (2017). НАУЧНОЕ НАСЛЕДИЕ ХАКИМА ТИРМИЗИ И ИССЛЕДОВАНИЯ ЕГО ТРУДА" ХАТМ-УЛ-АУЛИЯ"(“ПЕЧАТЬ ДРУЗЕЙ БОЖЬИХ”). In EUROPEAN RESEARCH (pp. 24-27).