International Journal of Political Science
ISSN: 2228-6217
Vol 12, No 1, January & February 2022, (pp.55-70)

Pathology of the New Cyber Terrorism Threat to Iran's National Security

Reza Solgi[1], Hassan Khodaverdi[2*], Zohreh Poustinchi[3]
[1]PhD Candidate in International Relations, Islamic Azad University, South Tehran Branch, Tehran, Iran
[2*,3]Department of Political Science and International Relations, South Tehran Branch, Islamic Azad University, Tehran, Iran

Received: 22 Nov 2021 ; Accepted: 21 Jan 2022

Abstract:
Cyber terrorism is one of the negative consequences of the information and communication technology revolution, which has been committed by individuals, governments and even organized terrorist groups with various motives and goals and has endangered the life and security of human society. Hence, today, cyber terrorism has become one of the main threats to the national security of countries. Meanwhile, the Islamic Republic of Iran is one of the countries whose threats in cyberspace, due to the widespread use of the Internet, network and cyberspace, has risen to the top of security threats in this country. The purpose of this study is to use the descriptive-analytical method to test the hypothesis and the library and fish-taking method for data collection, along with the use of Castells network theory, to answer the question that What impact does cyber terrorism have on the national security of the Islamic Republic of Iran? The results of this study indicate that the country has always been the target of numerous terrorist threats in the field of cyber in the last two decades ago. Creating public panic in society, assassination and physical elimination of elites and scientists using cyber technology, widespread exploitation of malware to damage and destroy vital infrastructure, theft of confidential information of government and citizens and its dissemination in cyberspace, public opinion management and the incitement of anti-government groups has been one of the most important threats of cyber terrorism, which in the past few years has caused extensive material and moral damage to the Islamic Republic of Iran and its citizens, and has posed serious challenges to its national security.

Keywords: Islamic Republic of Iran, Network Society, Cyber, Cyber Terrorism, National Security

*Corresponding Author's Email: h_khodaverdi@azad.ac.ir

Introduction

Today, the positive and negative effects and consequences of the information and communication technology revolution can be seen in all aspects of human life and relations between countries. The importance of this issue is such that understanding the nature of such an atmosphere in relation to the concept of national security and security of citizens is one of the most important perceptions necessary for different societies in the present age. Terrorism is not a new phenomenon and history is full of sinister terrorist acts that have been committed with various motives and have taken the lives of countless innocent people and endangered the rights, freedoms and security of the people. One of the negative consequences of information and communication technology is the change in terrorism, which has entered a new typological dimension by entering new areas affected by the information and communication age and has emerged under the title of "new cyber terrorism".

The features of information technology, especially the Internet, make it possible to organize and prepare organized cyber-attacks from long distances against predetermined targets and to terrorists in cyberspace allows them to act against their predetermined goals and cause disruption or destruction. It can be said that the emerging field of cyber has created the possibility of criminal behavior that has not been possible before. In this area, the whole of human society, from the individual to the largest international institutions can be considered the source of cyber terrorism. Hence, today, cyber terrorism has become one of the main threats to the national security of countries. The Islamic Republic of Iran is one of the countries that carries out most of its economic, commercial, cultural, social and governmental activities and interactions at all levels, including individuals, non-governmental organizations and governmental institutions in cyberspace. This country, as the axis of confrontation with global arrogance, has always been one of the main goals of the world's intelligence and terrorist organizations in cyberspace.

Hence, it has tasted the bitter taste of the devastation and damage caused by cyber-attacks, especially from the United States and Israel and organized terrorist groups. Therefore, today, the threat in cyberspace has risen to the top of the security threats of this country. Given the importance of a comprehensive and accurate understanding of cyberspace and terrorist threats affected by this space against the Islamic Republic of Iran and the study of appropriate and effective defense strategies against this threat, so this question arises what effect does the new cyber terrorism have on the national security of the Islamic Republic of Iran? In order to answer the research question, the hypothesis is raised that due to the vital activities of the Islamic Republic of Iran and even the lives of the citizens of this country to digital and computer systems, any disruption and damage to these systems in cyberspace can affect social order and national security. Descriptive-analytical method was used to test the hypothesis and library and fish-taking methods were used to collect data and information.

1-Background

Cristiano and others (2021), in an article entitled "Cyber Terrorism and Information Security in National Policy and International Diplomacy", examines the evolution and overlap of national policies and international diplomacy in the field of cyber terrorism. One of the strengths of this study is the study of international preventive laws under the

guidance and supervision of the United Nations, and the emphasis on preventing the activities of authoritarian regimes to exploit this technology, to strike at domestic opponents and international groups. Checkpoint Research (2021) in an article entitled "Indra - Hackers are behind the recent attacks on Iran" examines the widespread cyber which attacks on the systems of the Ministry of Roads, Urban Development and Railways of the Islamic Republic of Iran on July 9 and 10, 2021. The results of this study indicate that these attacks have relied heavily on the attacker's prior knowledge and identification of target networks. The attack is linked to a threatening non-governmental group that identifies itself as an opposition group to the Iranian regime called Indra.

Kaminsky (2020) describes in the article "Operation" Olympic Games "Cyber sabotage as a tool of the American intelligence community to thwart Iran's nuclear program", the US cyber operation against Iran, which in 2006 with the code of the Olympic Games and began under the leadership of the Bush administration. The results of this study indicate that the complex operations of cyber sabotage and thus the destruction of important infrastructure of a country on a large scale, requires the involvement of multiple government resources and advanced cyber activities and the use of various methods and extensive information resources. Fixler (2020), in an article entitled "Cyber Threat to Iran after Soleimani's Death", examines Iran's actions and cyber which attack against the United States after the assassination of General Qasem Soleimani by the US military. The results of this study show that based on Iran's past behavior and use of cyber as a tool in its asymmetric arsenal, Iranian-backed hackers are likely to attempt in the future to organize substantial cyber operations against critical US infrastructure. Yari (2020) in an article entitled "Cyber terrorism against Iran and strategies to combat it", points out that cyber which attack due to the comparative advantage of these attacks, reduce the cost of attack and its far-reaching consequences have always been the focus of the enemies of the Islamic Republic of Iran. One of the weaknesses of this study is that it mentions cyber threats against Iran in a very small and occasional way and the impact of these threats on Iran's national security was not analyzed.

Abed (2018) in an article entitled "Cyber terrorism, an emerging manifestation of terrorism", points out that today, along with all the benefits of computers and the expansion of cyberspace, cybercrime also appears as a new phenomenon. So that this space in the present era is a useful and safe tool for terrorists. One of the strengths of this research is the study of legal solutions to combat cybercrime. One of the weaknesses of this article is that a large part of this research is devoted to definitions. A review of the background of the research shows that many of these researches have only examined the criminal aspects of the use of cyber technology under the title of cyber terrorism or have examined the legal aspects of this issue. Or they have very superficially mentioned the impact of cyber terrorism on Iran's national security. Therefore, the leading research tries to examine the nature of cyber terrorism and the pathology of cyber terrorism against Iran's national security in detail.

2 - Theoretical framework (Castell's network community)

In order to study each phenomenon and reality, it must be placed in a coherent framework or format so that the subject under discussion can be examined in a coherent and systematic way and the connection between its different

parts can be shown. The content and philosophy of the new space, which is called cyberspace, is very different from the past and therefore can't be analyzed based on theories, approaches and levels of the past. In this new atmosphere, new and different types of friendship, cooperation, competition, enmity and war have been created along with the previous patterns. At the same time, various actors have been added to the traditional actors, which are very vague and unpredictable. As a result, a new theory and perspective must be emphasized that is much more flexible and open than in the past. On the other hand, addressing the issue of information and communication, and the impact that these technologies have had on various political, military, economic and cultural areas of different societies. Today, it is one of the most important ways to cure problems and the central symbol of the age in which we live. Thus, for the past few decades, many humanities thinkers, including Manuel Castells, have sought to describe "information and communication technology" as the defining feature of the new world. In this regard, for the first time in 1997, the term "network society" was introduced into the academic literature by Manuel Castells. (Asgar Khani et al., 2014, p. 82).

Castells is one of the sociologists who have been able to conceptualize the developments of modern society resulting from the development of information technology, including mobile, Internet and mass communication networks, and provide an independent and relatively comprehensive methodology. (Mazarr, 2002, p. 5)

The increasing development of information and communication technology, which Manuel Castells refers to as a networked society, has brought about a change in human life in various political, security, economic and social dimensions and has led to the emergence of a networked society. This development has been named the "Third Industrial Revolution". (Bell, 2007, p. 59) A global networking community is one in which social structures are formed around networks activated through information, communication, and digitally based microelectronic processing technologies. (Castells, 2014, p. 83)

Accordingly, according to the propositions and components that have been addressed in the theory of network society, Therefore, in this study, our reliance on the pathology of the new cyber terrorism threat on Iran's national security is the use of Manuel Castells's network community theory.

3 - The nature of cyberspace

Cyberspace is an area of operation whose framework is determined using electronic science to exploit information through interconnected systems and related infrastructures. Cyber is defined as the impact of space and society formed by computers, information and electronic devices, digital networks or their users. (Sharp & Lord, 2011, p. 10) Technological approach to cyberspace deals with components such as hardware, software, quality and quantity of data transfer and network interaction. The US Department of Defense defines cyberspace as a global realm in an information environment composed of an interconnected network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, processors, and embedding controllers. (Libicki, 2009, p. 6) In this regard, cyber which attacks refer to a group or many acts committed by hackers, which are sometimes accompanied by violence or severe effects. Of course, cyberattacks can have different criminal approaches. Sometimes these attacks

are preliminary and are carried out to obtain information and data to commit cybercrimes, and sometimes these attacks are directly within the framework of a cybercriminal description and the cases are called "cyber terrorism". (Khalili Pour and Noor Alivand, 2012, p. 169) Today, the main actors in network wars are terrorist communities and criminal and extremist groups that have an internal network structure and coordinate their operational and management nuclei remotely through communication technologies. (Federoff, 2006, pp. 34-35)

4- Cyber terrorism

Terrorism is not a new phenomenon. It can be said that it is as old as human social life. According to the Abrahamic discourse, Abel was the first victim of terrorism. Terrorism usually occurs in an environment where power is unfairly distributed. (Naji Rad, 2008, p. 7) There can be no definition of terrorism that covers the various forms of this phenomenon that have occurred throughout history. Encyclopedia Britannica defines terrorism as the systematic use of unpredictable intimidation and violence against governments and individuals to achieve a political goal. (New the Britannica Encyclopedia, 1986, p. 213)

Sharif Basyouni has offered another definition of terrorism. According to him, terrorism is: "Individual and collective coercive behavior by using strategies of violence, mixed with intimidation, which includes an international element or is targeted against an internationally protected target, and Its purpose is to achieve a power-hungry result. (QurbanNia, 2004, p. 144) Although information, communication, and media technologies were first developed and used by governments, especially the military. Gradually, however, after World War II, and widely since the beginning of the last decade of the twentieth century, and especially in Western democracies, it has penetrated deep into human societies and strengthened the emergence of political, social, economic and cultural movements.

Although governments were once the center of command for terrorist phenomena, today the threat of cyber terrorism as a substitute for revolutions, wars, with the transfer of power from governments to socio-political movements whose infrastructure is information technology, communications, and media and modern coups are based on these movements. (Naji Rad, 2006, p. 165) One of the first cyber-attacks took place in the mid-1970s during the Cold War between the United States and the former Soviet Union. But in most documents, "Kosovo" is cited as the first cyber war. The proliferation of cyberspace, which has intensified since the 1990s, has made it possible for terrorists to achieve their goals. The presence of millions of users in the virtual world, along with many companies, factories and major industries, which in many cases have high vulnerability, has increased the risk of cyberspace abuse and has also increased its attractiveness. (Kadkhodaei and Saed, 2011, pp. 72-73)

The term cyber-terrorism was first coined by Colin Barry in 1980, and a more comprehensive definition is provided by Ms. Dorothy Denning, Georgetown University Computer Science: "Cyber-terrorism is more about attacking or threatening computers, computer networks and information stored on them in order to intimidate or force the government or its citizens to advance specific political or social goals." (Seddon, 2004, p. 20) In another definition, cyber terrorism is the use of the Internet and computer networks and the facilities that these networks create with the aim of destroying the infrastructural

structures of society, such as energy, transportation, government activities, and influencing the government, Citizens and groups. (Abbasi, 2004, p. 30) In fact, terrorists, regardless of the nature and purpose of their actions, have very harmful and sometimes irreparable consequences. Usually, they target the critical points of the communities in order to inflict the most fundamental blows on their enemies and make the best use of the current situation, which is undoubtedly one of the best critical and infrastructural infrastructures. These groups are always equipped with the most advanced tools to achieve their sinister goal. One of the best tools is cyberspace. For an attack to be considered cyberterrorism, it must lead to violence against persons or property, or at least cause so much damage as to cause panic. Attacks that cause death, bodily injury, explosion, plane crash, water pollution or severe economic damage are among the cases. (Walker, 2006, p. 633)

The evolution of cyber technology is complicating capabilities over time. But these are relatively cheap. Like smartphones, online maps and Internet infrastructure are used as important components of combat operations along with other methods. The potential of using Internet networks and mobile information systems and intelligent technologies is very effective in facilitating terrorist attacks in cyberspace. (Livingstone & Cornis, 2010, p. 8) Cyber-terrorism differs from other terrorist tactics in that its existence is entirely dependent on the computer. (Hajiani and Zamiri, 2010, p. 40) Today, cyber terrorism is more dangerous than traditional terrorism, due to the growing economic structure and services of many countries based on information and communication technologies. (Sadoughi, 2001, p. 31) It can be said that the most important tool of cyber terrorists is the computer. In fact, they prefer to use bytes instead of bombs. (Seddon, 2004, p. 20)

Cyber terrorism has two main components:

1- Terrorists use computers to carry out non-violent activities that, although far removed from terrorism, facilitate it. A very common example of this is the use of the Internet for advertising and counter-information purposes.

2- Terrorist activities in which computer technology is one of the specific threats of a terrorist attack (either as a weapon or as a target). (Fleming and Stone, 2005, p. 131)

The difference between conventional terrorist tactics and computer-based tactics can be summarized in three key points: Facilitate operations, increase potential, and remain anonymous. The actions taken by these methods are not easily detected and can't be easily countered. Therefore, it enables terrorists to use computer technology to create sustainable support structures that help them advance their strategic and tactical goals. (Hajiani and Zamiri, 2010, p. 41) In general, it can be said that cyber terrorism attacks have unique features. On the one hand, these threats cover a wide range of legal, technical, organizational and cultural barriers and on the other hand, features such as ambiguity and uncertainty of cyberspace; Lack of adherence to a moral, value or normative framework; Easy access to cross-border and global information at low cost; Multiplicity of actors and dispersion of power in cyberspace; Low entry fee, low time spent and high speed of action; actors' anonymity and inability to track; amazing impact; The diminishing role of geography and the low probability of punishing or prosecuting criminal acts in cyberspace have led to many actors entering

this field. (Azimi and Khoshnoodi, 2016, pp. 163-164)

5 - Terrorist threats against the Islamic Republic of Iran in cyberspace

In political science, "power" and "security" are two completely interdependent concepts, and it can be boldly said that one might find a thinker in this field who denies the interdependence of these concepts. In recent centuries, changes in the concept of power and related resources have led to changes in the concept of security and related developments. In the new era, following the revolution in information, it seems that once again the sources of power in countries have undergone a profound transformation, which in turn has changed the concept of security. (Rosenau, 2011, p. 362) The ability to use cyberspace is one of the most important sources of power in the 21st century. Governmental and non-governmental actors use this power to achieve their social, ideological, political, military and financial goals in cyberspace and the real world. (Sharp & Lord, 2011, p. 22) The digital world, because of its cheapness and widespread access to information technology, has provided considerable potential for even the poorest governments and regional and global actors that may be used to challenge and threaten others. This contrasts with the important military technologies of the industrial age. In the information age, hardware and software are widely available and easy to use. In this age, governments are not the only international actors who may develop technical capabilities to use for harm; Rather, multinational corporations, NGOs, criminal and terrorist groups, and even individuals may engage in cyber warfare. (Alberts and Pope, 2006, p. 45).

The entanglement of today's world in the age of communication and information technology, along with the unique opportunities it has created, has raised concerns for countries with this technology. The Islamic Republic of Iran is no exception to this rule. One of the major concerns of the Islamic Republic of Iran is national security issues, which are severely threatened by cyber activities such as cyber terrorism. In the current situation, the Islamic Republic of Iran is facing a series of unspecified threats in cyberspace that have challenged the national security of this country and the traditional tools of providing national security of the Islamic Republic of Iran are no longer able to deal with these new threats. At present, most of the economic, commercial, cultural, social and governmental activities and interactions of the Islamic Republic of Iran at all levels, including individuals, non-governmental organizations and governmental and governmental institutions, are carried out in cyberspace. Vital and sensitive infrastructures and systems of the country, either form a part of the cyber space of the country or are controlled, managed and exploited through this space, and most of the vital and sensitive information of the country is transferred to this space or basically in this space is formed. Major media activities are transferred to this space, most financial exchanges are done through this space and a significant proportion of citizens' time and activities are spent interacting in this field. A significant part of the material and spiritual capital of the country has been spent in this field and a significant part of the material income and spiritual acquisitions of citizens have been obtained from this field or will be greatly affected by it. In other words, different aspects of citizens 'lives are literally intertwined with this space, and therefore any instability, insecurity, and challenges in this

area will directly endanger different aspects of citizens' lives. (Passive Defense Organization, 2015, p. 4)

5-1 - The role of the United States and Israel in organizing cyber terrorist attacks against Iran

Cyber terrorism against the Islamic Republic of Iran began in large part in a covert campaign code-named "Olympic Games" in 2006 under the leadership of the George W. Bush administration, which was initially targeted the Islamic Republic of Iran's nuclear capabilities. The next president of the United States, Obama, also expanded the Olympic campaign to include the use of offensive cyber weapons against Iran's nuclear enrichment facility. (Kaminski, 2020, pp. 64-70) But the most important threat of cyber terrorism against Iran using malware was the "Nitro Zeus" project under Barack Obama, which, if implemented operationally, could have completely disrupted important parts of Iran's economic and social infrastructure. According to the project, cyber and electronic equipment were deployed in Iran's computer networks, and if the nuclear talks between Iran and the United States failed, all of these tools would be used as a ready-to-serve army. This map was specially designed using malware to disable the computer systems of Iran's industrial and nuclear power plant sites. (Sanger, 2016, p. 6)

Israel has always been one of the newest enemies and opponents of the Iranian government in all areas, including cyber. It strongly emphasizes information cooperation with the United States, and therefore, along with the United States, has always strived to become a pioneer and leader in the field of cyber. This superiority is expressed in Netanyahu's speech at the "Cyber Week 2017" meeting. Emphasizing Israel's leadership power in the cyber world, Netanyahu called the country in a unique position relative to its size, saying: "Our small size does not geographically limit our cyber capabilities. It is the opposite. Because we are small, we are strong. I had set a goal to become one of the top five cyber powers and we have achieved that goal. His last sentence somehow indicates Israel's dominance in cyberspace. "We can hit someone 200 times bigger than ourselves," he said, noting that one-fifth of the world's cyber investment is made by the country. "There are things here that cannot be expressed in appearance." As a result, the Israeli prime minister's words, if true, indicate that the country has powerful cyber weapons that can somehow subject a society's vital infrastructure to "cyber sabotage" or "paralysis of infrastructure" by cyber terrorism. Israel's cooperation with US could be a continuation of broader operational plans against the Islamic Republic of Iran. Especially since the United States has also pursued a policy of cyber-aggression to deter. (Zanjani, 2019, p. 154)

5-2 - Division of cyber terrorist threats against Iran

Given that most of the important governmental and international affairs of the Islamic Republic of Iran and even the personal affairs of the citizens of this country are done in cyberspace, so any security threat posed by cyber terrorism can jeopardize the vital interests and national security of this country. The most important of these threats are the following:

5-2-1 - Creating public concern and fear in society

In times of war or crisis, the enemy can launch massive uprisings and subversions by relying on information gathered to attack crit-

ical infrastructure, or by tarnishing the credibility of information systems with public opinion and creating public concern. One of the features of information technology and cyberspace is the possibility of organizing and preparing an organized attack from a distance against predetermined targets. Which can even interfere with, prevent a proper defensive reaction or delay them. (Hassan Beigi, 2004, p. 13) Terrorists can use computers to create fear and panic among the people, and by disabling the technical facilities, they can damage the computers on which the economic, social, cultural and political life of the government and the people depend, on a large scale. And in this way, and through the threat of further attack, to gain points from their opponents. Today, the world of computers, which is related to people's lives, is a world that is threatened by terrorists at any moment, and this worry and the possibility of this happening is causing more and more people to fear and panic. (Tayeb, 2003, p. 89) For example, on July 9 and 10, 2021, Iran's railways and the systems of the Ministry of Roads and Urban Development were subjected to a widespread cyberattack. The research company "Research Point Check" examined this attack and found numerous evidence that show that these attacks rely heavily on the attacker's previous knowledge and identification of the target networks and are tactically and technically like the attack from 2019 which has also been carried out against several private companies in Syria. These activities are related to the non-governmental group that introduces itself as an opposition group to the Iranian regime called "Indra". The truth is that there is no magic shield that can prevent a type of destruction and damage to a country's vital infrastructure by cyberattackers. (Point Check Research, 2021, p. 1).

5-2-2 - Destruction of vital and sensitive systems and infrastructure using malware

Major weapons of cyber terrorists today include Trojan horses, viruses, computer worms, service blockers, password theft tools, and other malware. In 2010, a virus called Stuxnet was detected by the anti-virus Vba32, which spread rapidly in all countries of the world, especially Iran. The first time that the US cyberattack on Iran was seriously discussed was in August 2010 when it was announced that the US had used the Stuxnet virus to attack the computer systems of Iran's nuclear facilities. The complexity of the Stuxnet worm was so great that some experts referred to it as "cyber terrorism". Some even referred to it as a "weapon with extensive effects." It is said that this was the first computer virus designed to bring about physical change in the real world. The operation is in fact the first sustained US cyberattack against another country, using malicious code designed in collaboration with Israel. (Richardson, 2011, p. 13) About two years after the arrival of the Stuxnet virus, this time Iranian computers have been widely attacked by the flame virus. This sophisticated and advanced malware has been able to steal any information from the victim's computer. The Viper virus attack has been one of the largest cyberattacks against Iran over the past few years, resulting in irreparable damage to the information, systems and infrastructure of the Iranian Ministry of Oil. (Vaezi Nejad, 2012, p. 3).

Doku virus has also infected at least two telecommunications companies, an electronics maker, a cyber security company and venues hosting Iran's nuclear talks in recent years. (Constantin, 2015, p. 2) Malware such as Stuxnet, Flame, Doku, and Viper are just a few examples of terrorist attacks in cyber

space against the Islamic Republic of Iran under the large US-based Nitro Zeus project. The destruction of nuclear technology infrastructure using cyberspace under the guise of cyber terrorism has, to a large extent, led the United States and Israel to pursue their goals of weakening the Islamic Republic of Iran in the region and preventing it from playing a large role in neighboring countries. And this, without any hardware action and using spy-destructive malware, helps them achieve their strategy.

5-2-3 - Psychological terrorism and public opinion management

Psychological terrorism is another method in cyberspace to strike at the system of the Islamic Republic of Iran. "Terrorists are trying in cyber environment" by launching virtual social networks and publishing some provocative content, to stimulate popular demands and even ethnic movements in Iran. Accordingly, they are trying to use weapons such as propaganda, gossip, spreading lies and disturbing the public mind and targeting the belief system, intellectual foundations and psyche of the people, by intelligently and purposefully combining issues related to the demands of the people to wage a soft war with the Islamic Republic of Iran for its political and ideological goals. Thus, by inciting popular demands through virtual social networks, they have tried to create psychological insecurity in Iranian society and intend to turn this issue into a tool of deception and mental tension for the Iranian people. This action can help dissident groups to use virtual networks to attract public opinion and attract new forces and political-combat cadres, legitimize, oppress and present a strong, powerful and mythical image. And with the intensification of the feeling of insecurity among the citizens, along with lowering the threshold of tolerance of the people, panic, mentality and inducing the uncontrollable nature of the attack, and thus dragging the Iranian government to a security impasse, political blackmail and strike at the political system of the Islamic Republic of Iran. In cyber terrorism, it is possible to increase the ability to deceive and manipulate by relying on information techniques, so that images are presented that are completely different from the existing realities of a society. The truth is that there is an opportunity for terrorist elements to manipulate public understanding with the help of key information, thus steering public opinion in the desired direction.

5-2-4 - Deprivation of life of elites and scientists

The importance of this issue is such that even in general international human rights instruments as well as the experience of human rights courts, some theoretical issues on the issue of the right to life and its deprivation have been raised and emphasized. In this regard, not only are governments barred from depriving individuals of their right to life, but they are also obliged to eliminate any violation of their rights in the first place, and even to take precautionary measures to eliminate their lives. Meanwhile, the state and organized terrorism of the United States and Israel, by cleverly exploiting cyber technology, has deliberately assassinated the elites and nuclear scientists of the Islamic Republic of Iran, depriving them of the right to life. And in the last case, with the assassination of Martyr Mohsen Fakhri Zadeh as a nuclear scientist and official and government official, have violated human rights and the UN Charter. Currently, one of the reasons for the increase in terrorism is the development of the mass media and the widespread use of it by terrorists to intimidate countries and their greatest tool for

brutal operations, as well as to legitimize their shameful acts.

4-2-5 - Organizing anti-Iranian political campaigns

The creation of Internet political groups that are either not ostensibly affiliated with a particular institution or political group, or have concealed this issue, is a tool of psychological terrorism against the Islamic Republic of Iran. Some prominent activists affiliated with these groups have clear anti-Iranian tendencies and lead a series of destructive activities against the Iranian political system. "Also, most of the Opposition groups living abroad, due to the lack of any communication tools to communicate with the Iranian people, use the Internet as the most important means of communication inside Iran."

4-2-6 - Cyber espionage and theft of confidential and sensitive information

Cyber espionage is another method of terrorists to confront the Islamic Republic of Iran in cyberspace. This phenomenon is generally introduced in the form of obtaining information through programs that enter people's personal computers through the installation of software or while browsing the web environment, and if the user is connected to the World Wide Web, the information on his computer hard drive is stored, and sent to their preferred databases. For example, the leak of Iranian military classified information on US websites in November 2009 is an example of US cyber espionage against Iran. It was announced at the time that some classified information about Iranian missiles, including the Hoot missile, had been posted on the Internet.

4-2-7 -Expansion of electronic civil disobedience

Electronic civil disobedience, which drives protests from the streets to cyberspace, is another method used by the enemies of the Islamic Republic of Iran to use cyberspace to confront the regime of the Islamic Republic of Iran. Virtual demonstrations, hacking into popular sites and posting pictures, news and political content against the government and the use of search bombs are among the most important methods of electronic civil disobedience, first perpetrated by a group called the Critical Arts Group in 1994 and in A book called Electronic Disorder was introduced. Part of the purpose of e-civil disobedience is the popular information struggle or the information struggle from below, in which it is not the government but the people who are directly involved in shaping the flow of information to fight the government or to protest social's problems. This struggle is merely a letter-based struggle in cyberspace, but it is an effective and main step towards the formation of a social movement and pressure on the governing body of the Islamic Republic of Iran. The above are just a few examples of the widespread cyber-terrorism attacks against the Islamic Republic of Iran, which in less than two decades have targeted the citizens of the Islamic Republic of Iran, from critical facilities to their private lives.

Therefore, it can be said that today the cyber security of the Islamic Republic of Iran is directly related to the national security of this country. National security can no longer be defined solely in relation to foreign borders and the protection of the lives of its citizens by the military. Nowadays, thanks to the Internet and a computer device, the enemy has infiltrated organizations, companies, facilities and even the homes of the citizens of the Islamic Republic of Iran without realizing its physical presence. Such a pervasive threat has called into question all common and traditional conceptions of the concept of national security. Therefore, achieving effective

government arrangements in this area, a comprehensive and inclusive strategy that includes coordinated actions by the government, the private sector and citizens, is more than ever necessary.

6 - Proposed measures to combat cyber terrorism

The Islamic Republic of Iran, like any other country, needs a comprehensive strategy to combat cyber-terrorism in order to ensure national security and achieve its vital interests, because its security environment poses numerous threats rather than opportunities. The events and consequences of the last decade against the Islamic Republic of Iran point to the fact that a large part of the threats against this country, especially in systems, critical infrastructure, have originated directly from cyberspace. Accordingly, promoting operational stability and security and securing infrastructure, especially vital and sensitive centers, is very important for the Islamic Republic of Iran. This issue increases the role of the Government of the Islamic Republic of Iran and those in charge in controlling, monitoring and ensuring the security of cyberspace. In this regard, gaining the deterrent power in the field of cyber, can be one of the effective factors in defending against cyber terrorism. In the process of preventing cyber-attacks, the Islamic Republic of Iran needs a multi-layered defense, which includes surveillance systems, procedures, policies, training and awareness, control and restriction of access, and physical security measures, etc. Risk analysis and identification of vulnerabilities in networks and all digital systems under the web and updating of all anti-virus software and firewalls can have a significant impact on the process of preventing intrusion and cyber-attacks on the critical infrastructure of the Islamic Republic of Iran. In addition to eradicating the causes of the boom in terrorism, we must seek to eradicate the causes of cyber terrorism, formulate separate and guaranteed laws, establish a virtual council in the country against cyber terrorism, cooperate with other countries and the international community in the fight against cyber terrorism.

Conclusion

The information and communication technology revolution in the last decades of the twentieth century has had dramatic and unimaginable effects on human societies. So that today human life is experiencing a new stage of its evolution. It can be said that the dominant functions and processes in the information age are increasingly organized around networks. In this age, Internet and cyberspace technology is one of the greatest technologies designed, engineered and implemented by humans. In cyberspace, presence is even beyond the World Wide Web or the Internet. This space is defined as the global realm of the information environment, which consists of an interconnected network of information technology infrastructures, including: the Internet, telecommunications networks, computer systems, processors, and embedded controllers. In this regard, Manuel Castells introduces the development of information and communication technology as the cause of change in human life in various political, security, economic and social dimensions and refers to it as a networked society.

The entanglement of today's world in this age, along with the unique opportunities it has created for different human societies, has also raised concerns. One of these concerns is the national security issues of nation-states, which are severely threatened by organized and destructive cyber activities. One of the

most obvious unequal threats in cyberspace is cyber terrorism, which includes all three sides of the triangle of government, nation and army. Cyber terrorism is the result of the intersection and convergence of the two words "cyber" and "terror" and while having unique features such as ambiguity of space, lack of adherence to moral, value and normative frameworks, multiplicity of actors, low cost, dramatic impact and Most importantly, the anonymity of the perpetrator, with various motives and goals, has been committed by individuals, organizations or governments, and even organized terrorist groups, and has endangered the life and security of human society. Hence, today, cyber terrorism has become one of the main threats to the national security of countries. Meanwhile, the Islamic Republic of Iran is one of the countries whose threats in cyberspace today due to the widespread use of Internet technology, network and cyberspace, has climbed to the top of security threats in this country. Using Castells's network community theory, this study sought to answer the question: What effect does cyber terrorism have on the national security of the Islamic Republic of Iran? The results of this study show that the Islamic Republic of Iran, due to its extensive activities and interactions at various levels of economic, cultural, social and governance in cyberspace, has always been the subject of widespread cyber-attacks in various fields by its enemies.

Organized governmental and non-governmental terrorists and even governments opposed to the Iranian regime during less than two decades ago, with the widespread use of Internet technology and cyberspace, several threats have been made to the national security of the Islamic Republic of Iran, the most important of which is to create public concern and fear in society; Deprivation of life of elites and scientists; Destruction of vital and sensitive systems and infrastructure of the Islamic Republic of Iran using malware; Psychological terrorism and public opinion management; Forming anti-Iranian political campaigns; Cyber espionage and theft confidential information and the spread of electronic civil disobedience noted. These actions have inflicted extensive material and moral damage on the Islamic Republic of Iran and its citizens and have posed serious challenges to the national security of this country. In order to optimally manage and control cyberspace and reduce vulnerabilities in the field of cyber terrorism, the Islamic Republic of Iran should try to eradicate the causes of the cyber terrorism boom, seek to root out the causes of cyber terrorism, develop separate laws and guarantee implementation in this area to form a virtual council in the country against cyber terrorism, to cooperate with other countries and the consensus of the international community to deal with this ominous phenomenon. The best way to deal with cyber terrorism is to further strengthen cyber security and defense measures.

References

Abbasi, Mehdi (2017). Internet is a tool of cyber terrorism policy; Threat to the Future, Journal of Culture and Technology, First Year, No. 3, pp. 25-42

Abed, Reza (2015). Cyber Terrorism, An Emerging Perspective of Terrorism, Tehran, Fifth National Conference on Criminal Law and Sciences, pp. 1-19

Alberts, David and Daniel, Pope (2006). Excerpts from the Information Age: National Security Requirements in the Information Age, translated by Ali Aliabadi and Reza Nakhjavani, Tehran: Institute for Strategic Studies

Azimi, Fatemeh and Khoshnoodi, Hadi (2016). The Role of Cyber Terrorism in Threatening Iran's Security and Ways to Prevent It, Quarterly Journal of Political Studies, Ninth Year, No. 34, pp. 159-172

Bell, David. (2007). Cyberculture Theorists: Manuel Castells and Donna Haraway. Routledge Press

Borghei, Seyed Mehdi (2014). A Review of Cyber Security; Lessons for the Islamic Republic of Iran, Quarterly Journal of Islamic Revolution Studies, Eleventh Year, No. 38, pp. 85-104

Castells, Manuel (2014). The power of communication, translated by Hossein Basirian Jahromi, Tehran: Institute of Art, Culture and Communication

Check Point Research. (2021). Indra-Hackers Behind Recent Attacks on Iran, at: https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran

Constantin, Lucian. (2015). Duqu spy group also targeted telecommunications companies, Available at: http://www.pcworld.co.nz/article/577233/duqu-spy-group-also-targetedtelecommunications- companies

Coronis, Paul & et al. (November 2010). "On Cyber Warfare", A Chatham House Report, at: www.chathamhouse.org.uk

Cristiano, Fabio & et al. (2021). Cyber Terrorism and Information Security across National Policies and International Diplomacy, Studies in Conflict & Terrorism journal, Institute of Security and Global Affairs, Leiden University, The Hague, The Netherlands, at: https://doi.org/10.1080/1057610X.2021.1928887

Federov, Alexander (2006). Mega Terrorism is a New Challenge in the New Century, translated by Shams Sadat Hal Etayi, Abbas Yaghoubifar and Mohammad Mansouri, Tehran: Rasha Publications

Fixler, Annie (2020). The Cyber Threat from Iran after the Death of Soleimani. CTC Sentinel, Volume 13, Issue 2, pp 1- 40

Ghorbannia, Nasser (2004). Response to Terrorism: Military, Political or Legal Approach? Journal of Comparative Law, 0(6), No 43, 141-168.

Hajiani, Ebrahim and Zamiri, Abdolhossein (2010). Terrorism Research and Studies, Tehran: Strategic Research Institute of the Expediency Council

Hassan Beigi, Ibrahim (2004). Law and Security in Cyberspace, Tehran: Abrar Moaser Publishing

Javaheri, Mehdi (2015). A Study of Terrorism from the Typological Study of Cyber Terrorism in the Discussion of Nuclear Technology in Iran, 64-

Quarterly Journal of International Police Studies, No. 24, pp. 31

Kadkhodaei, Abbas Ali and Saed, Nader (2011). Terrorism and countering it, Tehran: World Islamic Peace Forum

Kaminski, Mariusz Antoni. (2020). Operation "Olympic Games." Cyber-sabotage as a tool of American Intelligence aimed at counteracting the development of Iran's nuclear program, security defense, Faculty of National Security, War Studies University, gen. Chruściela "Montera" 103, 00-910 Warsaw, Poland, at: http://doi.org/10.35467/sdq/121974

Kaminski, Mariusz Antoni. (2020). Operation "Olympic Games." Cyber-sabotage as a tool of American Intelligence aimed at counteracting the development of Iran's nuclear program Security and Defense Quarterly, vol. 29(2), 63-71, at: https://orcid.org/0000-0001-9395-9744

Khalili Pour Roknabadi, Ali and Noor Alivand, Yaser (2012). Studies Quarterly, "Cyber Threats and Its Impact on National Security" 196- Strategic, Year 15, No. 2, pp. 1-19

Lisicki, Martin C. (2009). Cyber deterrence and cyberwar. USA: RAND Corporation

Lord, Kristin M. & Sharp, Travis. (2011). "America's Cyber Future Security and Prosperity in the Information Age", Center for a New American Security, Volume I.

Mah Pishanian, Mahsa (2009). Explaining Ethnic Conflicts Based on Intervention Theories: A Look at the Soft Threats of the United States of America to the Islamic Republic of Iran, Psychological Operations Quarterly, Volume 6, Number 24, pp. 119-151

Mashreq News Analytical Website (2019). Cyber war against Iran; From Bush to Trump, Available at; https://www.mashreghnews.ir/news/969235

Mazarr, Michael. (2002). Information Technology and world politics, New York: Palgrave Macmillan

Mohammadi Al-Mawti, Mohsen; Jalali, Mahmoud and Shoushtari, Mehdi (2017). The Right to Life and Its Deprivation from the Perspective of Islam and International Human Rights with Emphasis on Suicide Operations, Two Quarterly Journal of Religious Anthropology, Fourteenth Year, No. 37, pp. 143-165

Naji Rad, Mohammad Ali (2006). Globalization of Terrorism and the Reasons for Cooperation of Countries Against It, PhD Thesis, Faculty of Law and Political Science, University of Tehran

Naji Rad, Mohammad Ali (2008). Globalization of Terrorism, Tehran: Ministry of Foreign Affairs Publishing Center

Passive Defense Organization (2015). Mission, Objectives and Mission of Cyber Defense, PAPSA Monthly, No. 9, pp. 1-36

Peter, Fleming and Stone, Michael (2005). Cyber terrorism: Imaginations and Realities, translated by Ismail Baghaei Hamianeh and Abbas Bagherpour Ardakani, Tehran: Ney Publishing

Richardson, John. (2011). Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield, Electronic copy Available at: http://ssrn.com/abstract=1892888

Rosenau, James (2011). Information Revolution, Security and New Technologies, translated by Alireza Tayeb, Tehran: Research Institute for Strategic Studies

Sadoughi, Morad Ali (2001). Information Technology and National Governance, Tehran: Office of Political and International Studies

Sanger, David E. (2016). Obama Order Sped Up Wave of Cyberattacks Against Iran, Published: June 1, at: http://www.nytimes.com/2012/06/01/world/ middle east/Obama ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1and_r=3andseid=autoandsmid=tw-nytimestechand

Seddon, Embar. (2004). Cyber Terrorism, Edited Alan Oday, Ash gate publishing Company

Shademani, Yaser (2016). The Strategy of the Islamic Republic of Iran in Reaction to the Deprivation of the Right to Life in the Assassination of Shahid Fakhri Zadeh (Nuclear Scientist) Journal of Human Rights, Year 6, No. 3, pp. 11-29

The New Encyclopedia Britannica. (1986). Vole 11, Micropaedia

Vaezi Nejad, Mohammad Mehdi (2012). Viper virus, Qatreh news analytics site, available at: http://www.ghatreh.com/news/nn10109996

Walker, Clive. (2006). Cyber terrorism. legal principle and law in the United Kingdom, pen state law rev.110.no 3

Yari, Maryam (2016). Cyber Terrorism against Iran and Strategies to Counter It, Identity Letter, No. 60, pp. 48-52

Zanjani, Javad (2019). Identifying and Dealing with the Cyber Threats of the Zionist Regime against the Army of the Islamic Republic of Iran, Master Thesis, Faculty of Command and Staff of the Army of the Islamic Republic of Iran

Ziaee Parvar, Hamid (2010). Post-Election Cyber Warfare, Tehran: Abrar Moaser Publishing.