International Journal of Political Science
ISSN: 2228-6217
Vol 11, No2, Summer 2021, (pp.23-38)

Recognizing the Effects of Cyberspace on International Peace and Security in the Age of Globalization based on Castells' Theory

Qasem Ranjbar[1], Mohammad Abbasi [2*]

[1] Department of International Relations, Islamic Azad University, South Tehran Branch, Tehran, Iran

[2*] Department of Political Science and International Relations, Farabi Faculty of Science and Technology, Tehran, Iran

Received: 11 May 2021 ; Accepted: 13 June 2021

Abstract:

Manuel Castells, a leading theorist of communication science, describes the Internet as a hallmark of communication technology called a Networked Society whose fundamental principle is the importance of individual centrality in various fields using new communication and information tools is called Cyberspace. In fact, in the age of Globalization and Cyberspace, many components of International Peace and Security have changed. Before the recent developments in international relations, peace and security meant respect for the principles of sovereignty, respect for the territorial integrity of countries, non-interference in each other's internal affairs, and the peaceful settlement of disputes, but now Cyberspace and Globalization have changed the concept of international peace and security. Therefore, to investigate the effects of Cyberspace on international peace and security in the age of globalization and use descriptive-analytical methods and library studies, the author seeks to analyze this issue and the findings indicate that in this period In addition to the new interpretation of international peace and security and its impact on the concepts of power, sovereignty, and security, the nature of threats has also changed and extended militarily to other areas such as cyber terrorism, soft war and so on. As a result of the development and expansion of Cyberspace and its tools in the form of networks and virtual media, a great change has taken place in the field of national security of governments, which has also affected international peace and security.

Keywords: Cyberspace, International peace, and security, Globalization, Cyber terrorism, Soft warfare.

[*] Corresponding author's Email: ma10773@gmail.com

Introduction

In recent years, "information and communication technologies" have expanded and this has affected human life in various dimensions, including political, social, and cultural. Communication technology and its dominant aspect, that is the Internet, have undergone unprecedented changes in our age; So that it has become the most dominant aspect of the contemporary world. Manuel Castells refers to it as a "network society" (Castells, 2006: p.15) which has led to change in various political, security, economic and social aspects.

This network society with features such as information economy, virtual culture, and reducing the importance of time and place in social interactions, has given a unique feature to the third millennium, that its fundamental principle is the central importance of the individual's presence in the field of social, political and economic activities, using new communication and information tools.

In such a space that is described as cyberspace, the set of human internal communications is formed through computers and related telecommunications devices, without considering physical geography. (Castells, 2001: p.553) In general, new information technologies connect all kinds of near and far parts of the world in global networks. Computer communications create a set of virtual societies, following which all human material and ideal structures and processes are transformed. (Castells, 2001: p.48)

On the other hand, today the first and most important goal of countries in international relations is peace and the establishment of peace and security.

Until before the emergence of recent developments in international relations, peace and security from the military point of view which is called the Westphalian system was regarded as an observance of the principles of sovereignty, equality of rights, respect for the immunity of states, and their representatives, respect for territorial integrity, non - interference in their internal affairs, and the peaceful settlement of disputes. (Ashrafi, 2014: p.83)

In this view, international security has received little attention, which was limited to the borders of states. From this point of view, the most important element of international security was the sovereignty and independence of governments. If there was a threat, it was mainly military, and these threats were usually from other governments. In addition, governments or their allies were primarily responsible for providing security.

Therefore, peace and security in international relations mean stability in the international community. Security is generally referred to as a kind of psychological feeling in which peace and confidence are achieved due to lack of fear.

Many different reasons may cause fear and disturb the peace, but the passing of time they change, because over time, the structure of human societies has become more complex and the interdependence of individuals and different societies has increased. (Ashrafi, 2014: p.84)

The phenomenon of globalization and cyberspace as a cause and effect of each other have caused changes in the present era and changes in the concepts of peace and security, and have given distinctive features to the third millennium. In other words, the emergence and expansion of information, electronic and media networks, and in more precisely the waves of globalization, show that a new and more complex period in international relations has begun. The new information and communication technologies, developed since the early 1990s on the global scale,

have accelerated institutional change, increased international interaction, and changes in the main concepts of political science and international relations, including threat, power, and so on.

Therefore, what is the place of cyberspace in today's world?! And how has it been able to change human life?! While it has made changes in the roots of economics, society, and culture, in a way that has achieved similar importance to the real world and is referred to as an independent indicator for defining a new era in the history of human evolutions and developments. The new era, of course, does not mean the complete loss of the past system;

The new world overlaps with the old world, and power is also dependent on geography-based institutions in this period. (Rezaei, 2012: p.2)

In any case, the result of such a space is the emergence of a world where the past traditional political boundaries are removed without the states getting involved in war and bloodshed and any changes that affect and transform our world. Thus, concerning the growth and development of cyberspace, we are observing its extensive effects on the process of power, sovereignty, and security, and finally the issue of peace and security in the international arena. So the main issue of this research is how does cyberspace affects international peace and security in the age of globalization?

Theoretical Foundations and Literature Review

Cyberspace

Cyber is a term derived from the word "kybernetes" and means steersman or guide. William Gibson, the author of science fiction stories, was the first person who uses the term of cyberspace, in the book of Neuromancer.

Some writers have defined cyberspace or virtual space as "a set of human internal communications through computers and telecommunications tools regardless of physical geography." Maybe it’s better to define it, like this:

“It is a real electronic environment in which human communication occurs rapidly, beyond geographical borders, with specific tools, and in a live and direct way”.

The adverb of "real" allows us to assume that the virtual nature of this space means that it is unreal; because this space also has the same features of human interactions in the outside world; while cyberspace is an environment where communications are formed, not only a set of communications. On the other hand, although these connections may not be online at all the time, they are live, real, and direct. Hence, this communication is effective. (Sediq Banai, 1385: p.3) Thus cyberspace is an electronic environment where a group of people meet and talk to each other. Technically, cyberspace is a type of information space, which connects to the mother of all networks, the Internet, through the computer systems of digital networks. In other words, any non-physical space that is created by "online" computer systems can be considered as cyberspace. In this regard, cyberspace has various effects on communities, in a real environment, so this space will appear with its set of advantages and disadvantages in society. Therefore, it can be said that these technologies are not just a tool, but also affect and overshadow human communication approaches, as well as his thought processes and creativity (Soltani et al., 2008: p.8) In other words, as for real space and cyberspace, it can be said that cyberspace is not a neutral space. This space consists of numerous opportunities and problems that individuals, groups, society, government, and

states are dealing with and can disrupt country security and order, etc. (Janparvar and Mosul, 2011: p.146)

Castells Network Society and Communication Power

According to Castells, we achieve a pervasive conclusion by examining the newfound social structures in areas related to human activity and experience. As a historical trend, the dominant functions and processes in the information age, more than ever are becoming organized around the networks. Networks constitute the new social appearance of our societies, and the development of network logic creates significant changes in the operations and outcomes related to production processes, experience, power, and culture. While in other times and places there have been a network form of social organization, the new paradigm of information technology constitutes the basis for its inclusive expansion, in the whole social structure.

Moreover, network logic creates a social movement that level exceeds the specific social interests that have been expressed by the network: the power of flows surpasses the flows of power. Absence or presence in the network and its dynamism against other networks are important sources of domination and change in our society. In this way, a society can be called a network society in which social structure is superior to social action. (Ameli et al., 2016: p.94) Castells considers network society as a product of three independent historical processes, which are as follows: the information revolution that enabled the emergence of network society;

Revision of the structure of capitalism and economy relies on centralized planning from the 1980s onwards, to overcome the internal conflicts of the two systems; and the cultural movements of the 1960s and it's a continuation in the 1970s, movements like feminism and environmentalism. (Kazemi Najafabadi et al., 2018: p.202)

In the three-volume book of the Information Age, Castells considers a network society as a new society in which "power communications", "production communications" and "experience" are formed around the network, indicating a new morphology of society. In line with his earlier approach, Castells seeks to explain power communications in a network society, in a more precise manner; he had talked about its changes in general. Castells' argument is based on the concept of a network society. According to Castells, a global network society is a society in which social structures are formed around the activated networks via digital information and communication technologies, and based on microelectronics.

In this society, the governance of networks is based on activities and people who are considered foreign relative to the networks, and in this sense, global networks lead to the destruction of local networks. In his definition of power, Castells refers to the two elements of "communication" and "meaning", and therefore Castells' attempt throughout the book is to show that the communication capacity is the most important factor that social actors possess and with its help and through the change in the process of semantics, they can influence the decisions of other actors. People who manage the communication capacity in the global network society are undoubtedly the owners of power in the networks. Castells has clearly explained the reason why:

The network is a communication structure between multiple points within a network or between multiple networks, and this communication structure consists of the patterns of contacts. So if you can control the communi-

cation issue in the network, you have the patterns of contacts, and that means the acquisition of power. Simply put, power in networks belongs to those who manage and control the communications and contact patterns between network points. (Divsalar, 2014: p.93-94)

There is one thing in common in Castells' theories, such as the theories of "network society" and the "power of communication," and it is an effort to prove the universality of these theories. However Castells tries to keep his distance from the beliefs of the modernist paradigm, but he agrees to this paradigm, which seeks to present universal theories. In the book "Power of Communication", Castells tries to prove that power and counter-power are embedded in the global communication networks: "Power is applied primarily through meaning in the human mind and with the help of communication processes which are implemented in the global/local multimedia networks with a mass communication approach, including Mass self-communication." (Castells, 2014: p.743).

"With the increasing influence of the Internet, a new form of interactive communication has emerged, and therefore the capacity to send many-to-many messages is specified in the present tense and with the possibility of using point-to-point communication, limited or extensive diffusion, and given the goals and features focused on communication action. I call this new form of communication historically "Mass self-communications". (Castells, 2014: p.144) Castells considers four types of power for the network: Networking power, Network power, Networked power, Network-making power (Ibid: p.117). In any case, Castells' main claim in the book "The Power of Communication" has two main aspects: First, the communication networks play a pivotal role in the rise to power of any network, including financial, cultural, industrial, political, and scientific networks, and communication networks are the main networks for creating power in society. Second, network programmers and "switchers" who can establish multiple connections between different networks are the main owners of power. Castells even considers the origin of the counter-power process in the network society as the reprogramming of networks around alternative interests and values, by interrupting the dominant switching process while switching resistance networks and social change. In this way, in his own words, he has replaced the property of communication tools with the property of the production tools, to be able to explain the nature of power in a network society. (Divsalar, 2014: p.96-98)

Globalization can be considered as a process or a set of processes that lead to a transformation in organizing the space of social communications that ensures the expansion of social, political, economic activities, and communication beyond the borders, regions, and continents. It can also relate the extent, intensity, and speed of global interactions to their expanding influence in such a way that its effects can be quite evident elsewhere, and in that sense the boundaries between domestic and world affairs are increasingly smoothed. Globalization can be regarded as the expansion, intensification, acceleration, and growth of the world.

Some have called globalization shrinking and approaching globalization. Some consider it as a spatial-temporal separation and some consider it as the expansion of capitalism or liberation from the domination of the state-nation. (Nosratinejad, 2002: p.142)

Terms such as "the interpretation of the world", "dependence of different parts of the world", "Increasing global dependence and entanglement", "The process of global wes-

1. According to Manuel Castells' theory, in a network society, power lies in communications, and the controllers of the communications flow, whom he classifies into switchers and programmers, are the owners of power.

ternization and assimilation", "Integration of all economic aspects in a global scale" and "Expanding the scope of the affectivity and impact ability of social actions", are some of the definitions of globalization. (Shahramnia and Nazifinaeini, 2013: p.144).

International peace and security

The first and most important goal in international relations is the maintenance of international peace and security, which is the responsibility of the Security Council, under Article 24 of the Charter of the United Nations. At present, even though there is no war between countries, but there may not be peaceful relations between countries, and this means that the concept of peace in international relations has changed. The word of peace means reconciliation, friendship, compromise, etc. In political culture, peace means feeling the calmness in normal relations with other countries and the lack of war and threat. Peaceful coexistence in relations between countries means observance of the principles of sovereignty, equality of rights, immunity, territorial integrity of each country, big or small, non-interference in the internal affairs of other countries, and terminating international problems. (Galtung, 1992: p.32)

But the term of security refers to a kind of mental sensation in which, a sense of calm and confidence is achieved, due to the lack of fear. In general, security refers to the avoidance of dangers that threaten human interests and values. After the conclusion of the Peace of Westphalia in 1648 and the formation of the nation-state system, the concept of national security was introduced in international relations, and the concept of international security has also emerged with the passage of time and the deepening of international relations. In the past, international security was commonly defined in the field of military security, but today it is defined in political, military, economic, and social dimensions. Since the concept of peace was limited, the concept of international security in the past did not go far beyond the borders of states and was based on the national security of states. Therefore, the independence and national sovereignty of states were considered the most important element of international security. (Ashrafi, 2013: p.86-87) Therefore, given the current situation in international relations and the changing world, the concept of peace and global security has two points to consider. First, international peace and security are not necessarily provided by the status quo; as the laws and legal structures of the ruling system, international relations may have a cruel and discriminatory nature.

Since peace is one of the concepts associated with justice, it cannot last without justice. Secondly, in the past, peace and security were some of the concepts that were used only in the military and political domain, but today, especially the term of security is used in political, cultural, economic, technological dimensions. Although military clashes and political conflicts are still the most important threat factors of peace and security, the interference of these territories, as one of the consequences of globalization has led to the crisis and insecurity in one domain be transferred to other territories. (Poorahmadi and Moradi, 2018: p.44).

Research methodology

In this article, we have used the descriptive-analytical method. Thus, in the theoretical discussion, the researcher has simply described the variables by extracting information from various sources and presenting them.

Then, in the findings section, he has analyzed the impact of the independent variable,

i.e. cyberspace, on the dependent variable and its components, namely international peace and security, power, sovereignty, threat, and security, as well as globalization.

In this regard, Manuel Castells' view has been noted due to its compatibility with the influential component of cyberspace on national security, as well as we have used it for content analysis, indirectly. Thus, in the end, in line with the purpose of this article, the conclusion is analyzed; Data is collected through library and internet studies and process analysis has been done theoretically.

Findings and data analysis

The influence of cyberspace and changing the concept and nature of power in the age of globalization

The globalization and revolution of information and communication have increased the importance of networks and changed the area of power. Networks are the same relationships, and different types of networks create different forms of power. Nowadays, in the information age, information control in networks is an important source of power, and centrality (greater number of internal and external links) in networks can lead to power generation. Information and knowledge are important sources of the implementation of power.

Hence, it is important to know that today, technology has changed social and political processes and has led to a shift like interaction and communication and the acceleration of institutional change in the international arena in economic, political, cultural, and social dimensions. Therefore, in the age of globalization, success in the management of these public and private networks depends on talent, environmental intelligence, and new forms of power (Nay, 2008: p.315-330).

In the age of globalization, power is gradually removed from the monopoly of government and official institutions and is available to national and transnational corporations and other non-national institutions.

Foucault speaks of the shrinking of power in the postmodern era. He believes that the centrality of power has disappeared and power has become individual. (Toffler, 1996: p.378) Suzanne Nossel explained the term "smart power" for the first time in Foreign Affairs magazine, resulting from a rational combination of soft power and hard power in the age of globalization. This intellectual combination is based on the type of threats, the sources of national and transnational power under the control, and the operational conditions of the target environment, and it is a time-consuming process that requires accurate, exact, and well-timed information from the opponent, threat environment and space, correct and accurate possibilities, capabilities and sources of potential and actual power, with the national and transnational origin;

Also, the rationality of the actors with accurate recognition of their capabilities and possibilities, the correct choice of possible tools for the exercise of power, the rational composition of tools, is an example of soft power and hard power, correct assessment of results and consequences, aiming to complete the effectiveness period to achieve the desired situation and intelligent leadership of the security environment, appropriate to the type, intensity, scope and consequences of the security crisis (Nossel, 2004). This is

while the importance of hard power based on top-down imposition is decreasing day by day. The development of resources and communication networks has made image control and management very important. According to Gallarotti, the world is becoming a softer world.

In such a space, the legitimacy and credibility of a country's foreign policy depend on

1. Centrality is a measure that quantifies the advantage of role-playing, supposedly an individual embedded in the network. In other words, the centrality measure attempts to measure a role-player.

the soft power resulting from the economic growth and democratic system. (Gallarotti, 2010: p.38)

The impact of cyberspace and changing the concept of national sovereignty in the age of globalization

The equip ability of the local systems is weakened because of globalization and the authority of nation-states is in danger. In this regard, by weakening the traditional authority and sovereignty of the nation-state, a certain dimension of globalization does not come into play singly, but all aspects of globalization are effective in this area, and every aspect of globalization tries to undermine the control of governments. (Taghavi, 2003: p.134) In undermining national sovereignty, there are sextet components of globalization, which are:

1- Increasing economic-cultural relations reduces the power and efficiency of governments at the state-nation level. Thus, governments cannot control the influence of current ideas and trends beyond the borders. As a result, the efficiency of national governments is called into question.

2- According to the increasing impact of transnational factors, the power of the national government is constantly decreasing. As a result, new actors such as transnational corporations are exposing in the international arena.

3. The international system imposes itself on the national states and in the first step these states are forced to adapt to the world system.

4. Governments tend to redefine their national sovereignty in the form of larger political units such as the European Community or similar or multilateral organizations such as NATO and OPEC, or international organizations.

5- The uncontested sovereignty of the global system affected by superior culture, threatens the independent national powers.

6- To establish a comprehensive political-legal order, conflict occurs. (Eftekhari, 2002: 43)

The impact of cyberspace and changing the concept of security in the age of globalization

The traditional perspective of security, also known as narrow security, had three main features:

1- State-oriented and that the state is the only reference in the security-related analyzes

2. Military threats and war are the most important threats to the security of the country

3. Threats against the security of states have an external aspect;

However, in neo-realist security studies, security is also related to the domain of citizenship and has a direct relationship with citizenship, and governments are committed to providing the security of their citizens against the threats of other governments. But it is still the source of external threats and the source of government security. The state-oriented security perspective considered foreign military conflicts and ignored domestic violence. The mere focus on foreign threats had caused that the security of the people to be neglected within the countries in this view. (Vosoughi and Bazvand, 2013: p.141)

Gradually governments have changed their definitions of security and therefore are committed to transparency and accountability more than ever; In fact, globalization shifts security from the state of government-oriented towards the security of non - go-

vernmental actors and international organizations, that this process has reduced the power of governments and removed sovereignty from its absolute state.

In addition, human security and sustainable security are posed as the main concepts (kohara, 2005: p.39-40). On this basis, we can say that globalization has affected the political, economic, social, cultural, and environmental domains and consequently has created new security crises in these areas, which have caused concern to governments and, as a result, committed them to redefine the concept of security based on new conditions. In general, there are two types of theorists in the case of the impact of information and communication technology or cyberspace on the concept of security. Some believe that this tool can best dilute the concept of security and replace it with the concept of peace, in the sense that it can give a positive and affirmative meaning to the concept of security. In this way, the concept of security leads to the security of companies, non-profit organizations, social movements, transnational networks, and individuals, so by changing the concept of security of actors, security also changes and the same actors are the supplier of security; But the main problem in this kind of definition of the change in the concept of security, under the influence with information technology, is that the information revolution turns security into a concern which is considered by all sections of society.

The second groups who are the classical realism theorists believe that although information and communication technology has spread, the classical concept of security, meaning government security, has maintained its position in military form and official information flows. (Eriksson and Giacomello, 2006: p.222-223) Although traditionalists reject the concept of security as a concept that should be changed and interpreted according to the conditions and adhere to their traditional definition, others believe that the concept of security should be more broadly defined to include new social, economic, and environmental threats and challenges.

Cyberspace and change of thread concept in the globalization era

One of the most important impacts of cyberspace on change of security concept has been creating different interpretations regarding a single phenomenon and making the concept of 'threat' distinct based on making mindset distinct against objectivity. Therefore, the abundance of media and virtual spaces has an important role as a threat factor or resolving a threat against another issue (Soltani Nejad et al, 2017: p.25). By expansion of cyberspace, we see that in the international relationships arena; threats of the information era are different from the threats of the cold war era. During the cold war era, a threat against nations was relatively concentrated on and emanated from a single source; it means that one of two sides or a single nation was involved whereas it was regarding a specific issue such as land or nuclear weapons. Hence, the security of nations is reflected in military and political securities. After the termination of the cold war; probabilities of conflict between superpowers, application of nuclear weapons, and struggles on land conflicts were decreased, but those are replaced with other kinds of threats which emanated from economic, political management, sciences and technologies, social stability, environment, terrorism aspects and so. Information revolution helps diversification of threats. During the cold war, it was a distance between potential and de facto threat and the threatened side had time to evaluate the

situation and making the decision. But, in the information revolution era; the velocity of data transmission becomes more than before, and interplay at the international level increases while potential threat factors against the security of nations expanded and their destructive force also becomes further (Sadat Hosseini et al, 2017: p.136). Cyber threats are new phenomena that emerged during recent decades in the globalization era and along with information technology change as well as expansion of world communications via wide internet network throughout the world in such a way that nowadays; the challenges of cyber threats are seemed important and complicated (Roknabadi & Nooralivand, 2012: p.168). Based on this situation, during the globalization era; we witness the changes in threat aspects where these changes have occurred in threat sources as well as the type of threats and the applied tools which all have been changed dramatically. Globalization makes nations and human communities aware of numerous security threats and susceptibilities which either were ignored or simply were not realistic. The globalization era causes the expansion of threatening issues circle and also fading of the borderline between external and internal threats and on the other hands; today we are faced to threat which are without borders. For fading of the borderline between external and internal threat, we should state that through new studies about security issues; it is said that we are living under those conditions that national security threats are not merely caused by the existence of hostile neighbors, but other issues such as economic recession, political suppression, cultural shortages and deficiencies, environmental corruptions, beyond borders terrorism, international organized crimes, natural disasters, diseases, and health problems are added to traditional external threats (Mohseni, 2018: p.116-117), while a threat within cyberspace would be complicated, multi-dimensional and intangible. Thus, threat factors or agents, threat tools, and threat aims will be changed. Governments are not any longer the only agents of threat in the global security sphere but information technologies and communications also provide the capacity of threatening global immensity and create insecurity at national and international levels for private actors. Furthermore, tools of threat are changing from military tools, force, and compulsion to exploiting those software tools which are based on information technology and communications. Aims of threat also are changing from hard issues such as land territory seizure and invasion, destruction of economic and commercial centers to some issues such as culture, public opinion, values, norms, social identity, and political legitimacy. This change is called "soft threat" and is based on exploiting software tools and soft components while empowering states to achieve desired results and objectives within a long-term period. Furthermore, although formed threats under cyberspace have diversified spectrum; but there are common features such as lack of government orientation, generality and comprehensiveness and . . . connect all of those (Sadat Mohseni et al, 2016: p.137).

Cyberspace and war inside the arena of national actors' activities, international relationships, and expansion of cyberspace at globalization era eclipse contrast issue and war in arena of international relationships in such a way that we witness a new type of contrast amongst national actors as well as other actors of international relationship arena under cyber war criteria which embraces different dimensions and formations comparing to whatever we have seen before. Cyber

war can occur without any physical attack, then depending on widespread software systems; it can be harmful to states under a war without any roughness. Cyber is used to explain those systems which utilize mechanical or electronic systems as a replacement to control and human supervision. The term 'cyber' in cyber war terminology includes the systems that utilize software as a 'control element' and apply that. By these descriptions, cyber war is an action or a measure of a government to make the enemy doing its demand through destruction or harming software control processes inside enemies' system. This war includes; cyber penetration, cyber manipulation, cyber-attack, and cyber ambush. This event as mentioned in the report of 'Dartmouth College', includes organized units within governmental territories which during defense and attacking operations utilizes computers to attack other computers and networks through electronic tools (Philips, 2011: p.2). Cyber war can be used to describe different aspects of defense and attacking against informative and computerized networks within cyberspace as well as eliminating the capacity of an enemy in doing so. Cyber war under a wide perspective means the occurrence of war within cyberspace. By this expression, cyber war includes defending informative and computerized networks, preventing informative attacks and eliminating the capacity of the enemy to do so, conducting offensive operations against enemy or informative victory in this arena (Hildreth, 2001: p.5). War in cyberspace is operated by those actors who set to use this space to achieve their political goals (Khalilpour Roknabadi & Nooralivand, 2012: p.171). As Richard Clarke argues; cyber war is a new format of fighting that we still are not able to understand perfectly while it is clear that in the current world, the battlefield expanded to cyberspace and it must be considered as the fifth war field along with traditional ground, air, sea, and space fields (Cornish et al, 2010: p. 12-13).

Furthermore, one of the most important aspects in the international arena of war and contrast under the light of the development and expansion of cyberspace is the formation of psychological war at its ground. In the current world, the most important aspect of cyber threats is their psychological dimension. Psychological operations within cyberspace include planned activities to transmit information and selected indices to foreign receivers where the goal is influencing feelings, motivations, thinking, and reasoning strength and finally to change the behavior of organizations, groups, and their wills. Moreover, it may be seen that designing information rubbery operations under cyberspace is conducted to generate agitation and anxiety. The term 'psychological war' is one of the frequent concepts in corresponding texts and negotiations of strategy makers, political theorists, security authorized persons, and experts in the domain of social sciences. For example, the US military defines this term in its combatant bylaws as: "Psychological war is a war which the most important goal of that is influencing ideas, feelings, wills and characteristic behavior of enemies, unaligned parties or aligned groups to maintain supporting national objectives and goals" (Khalili Joulorestani, 2017: p.157). Hence, the technological revolution in the domain of social communications causes accessibility facilities to access millions of people's thoughts and influencing those minds whereas the same easy access is the reason for the creation of much more extended causalities in this communication featured war comparing to military wars. Furthermore, the bullets of media are much more fatal than the bullets of con-

ventional weapons. Undoubtedly, nowadays the communication technology is one of the fundamental tools of policymaking. With this technology, it is possible to enter the political environment of states and change that towards their benefit. Communication technology provides mentioned ability to actors of international relationships domain to expand their maneuver field from national circle to the furthest international level and maintain their national interests through this communication war. Mass media in the current world, communicate subjective and unreal worlds to our real world and determine how world's people think about for example today coups d'état in the Philippines or tomorrow issue of the Ozone layer and the day after tomorrow Aids infection and next week another issue where all these agendas are determined for world's people by some people who have the control of mass media and cyberspace within the international arena. The role of news agencies and cyberspace specifically finds its real significance through a framework of the same highlighting activities (Bahmani, 2012: p. 86 - 87).

Cyberspace and national security threat by cyber-crimes and cyber-terrorism

Cybercrimes are internet-driven crimes that include the generated crimes in the cyber environment. This kind of crime embraces cyber-attacks by spreading viruses, browse engines' spiders or crawlers, electromagnetic pulses, worms and so … under economic, personal revenge against public figures and agencies motivations and other incentives. Amongst these crimes, the most dangerous one is cyber-terrorism which can be planned mostly under political incentives along with generating widespread destruction in infrastructures of a government. The Internet has been entered into the existing arena as a structure that is free of states' control therefore it does not only provide destructive tools easily to unsatisfied people but also its structure is a suitable environment for criminal activities. Some of these activities that are called cyber-terrorism have been extended dramatically in such a way that its expansion causes weakening defense capacities of companies and governments which are exposed to hazard (Jahangiri & Pourghassab Amiri, 2011: p.118). The simplicity of hiding the origin and source of cyber-attacks and the fact that cyber-attack against a country can be originated from other countries means that cyber-crime and cyber-terrorism are international threats (Saed, 2011: p.109). The characteristic of cyber-terrorism and its distinct and fundamental difference with traditional terrorism is how to use its tool. Cyber-terrorism is referred to as a new phenomenon that has occurred within a different environment than traditional terrorism. Exploiting a computer in a cyber-medium is a unique and specified feature of this occurrence and an independent title is assigned to it due to this feature (Saed, 2011: p.98).

To summarize the reasons for resorting to cyber-terrorism attacks are abridged as mentioned below:

1. Cyber-attacks are less expensive than traditional terrorism attacks;
2. Tracking this kind of attack is very difficult;
3. Terrorists can hide their identity and used a location to set attacks;
4. Physical barriers or checkpoints are not available;
5. These attacks can be planned and operate from everywhere around the world;
6. By using cyber-attacks, there is the feasibility of attacking several targets synchronously;

7. The impact of these attacks can be on a huge number of people (Jahangiri & Pourghassab Amiri, 2011: p.122).

Cyber-terrorism is using computer networks tools to destruct fundamental infrastructures such as energy, transportation, state operations or apply force or threat to a government or nation. The fundamental theory of cyber-terrorism is described as the states and nations as well as fundamental infrastructures are going to be more dependent on computer networks to do their jobs, new susceptibilities would be created and a major electronic Achilles' heel emerges. Enemies of a government and cyber terrorists can exploit these susceptibility points of states to penetrate weak and less immune computer networks and damage or even destroy fundamental applications. These infrastructures embrace the economy and also military domains of a government, which means that damaging the economic security of targeted government through injuring fundamental, economic, and informative infrastructures of a government and also corrosion of military capacity by damaging fundamental infrastructures (Structural and informative) of a government. Many believe that susceptibility of computer networks and susceptibility of fundamental infrastructures are the same and equivalent and also this susceptibility puts the national security of a government at significant risk. However, this context is not too amazing due to the emergence of computers and the internet not so long ago and its consequence of cyberspace formation. Nevertheless, many people also consider this belief to be false (James, 2002: p.24). After all these descriptions, cyber-terrorism is considered as a potential and de facto hazard for national security which ultimately weakens its power and strength.

Conclusion

Manuel Castells has provided a description and acceptable expression of the current world's technological changes and their impacts on community, economy, culture, politics, and nation-state institution along with emphasizing the fact that in the last decade of the twentieth century; the world witnesses important social, political and technological changes. His analysis of institutional, cultural, and technological changes in contemporary communities and emergence of new types of communities under the title of network communities and at a planetary level, formation of some kind of network globalization together with network economy and network government provides helpful insight of the world that featured with changes of basic information. Castells emphasize is on the role of communication strength in the formation of politics whereas caused politics to be merely a controversy within media-oriented games and only dispute to be governing symbols on medium. Hence, by the development of cyberspace and entrance to the globalization era, we witness a change in the domain of international relationship actors. In this space, the most important traditional concepts of political sciences and international relationships such as sovereignty, power, and security have been subjected to important changes. Security at its military dimension is extended to other aspects of the economy, environment, and also social security. Moreover, the concept of power in the globalization era is undergone fundamental changes due to media development and cyberspace and increase in penetration and impact domains on ideas of targeted communities under the format of soft power became under attention as a new form of actors' power within the internal era as well as international relationships. On the other hand, the

development and expansion of cyberspace and its tools under the format of networks and cyber media create a significant change in the national security of states which also has influenced international peace and security. Cyberspace as a double-edged sword in the forms of production tools and security threat within the national era and also international relationships is considerable. At the ground of this formation, crimes such as cyber terrorism are those problems which in addition to threatening the national security of political actors, influence international peace and security. Moreover, we witness the formation of a new type of war and contrast amongst political actors under the framework of soft war that influenced security broadened dimensions (Military, political, economic, social, and environmental) of political actors, and also its range of impacts are extending because of cyberspace development. Hence, cyberspace has become the most important tool of belonged challenge ability to sovereignty political territories, weakening the power of government, a decline of national sovereignty, changing national security culture into global security as well as political legitimacy through the empowerment of decentralized secularists and other actors and activists, thus has influenced international peace and security that is affected by liberal democracy.

References

Berlin, I. (1958). Two concepts of liberty. In Isaiah Berlin (1969), Four essays on liberty. Oxford: Oxford University Press.

Braman, S. (2006). Change of state: Information, policy, and power. Cambridge MIT Press.

Castells, M., & United Nations Research Institute for Social Development. (1999). Information technology, globalization, and social development. Geneva United Nations Research Institute for Social Development

Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the internet, international relations, and global security. Bulletin of the Atomic Scientists, 68(2). 70-77

Eriksson, J. Giacomello, G. (2006). The Information Revolution, Security, and International Relations. Relevant Theory. 27(3).

Gallarotti, Giulio M. (2010). Cosmopolitan Power in International Relations: A Synthesis of Realism, Neoliberalism, and Constructivism. Cambridge and New York: Cambridge University Press.

Galtung, Johan. (1996). The European Community: A Superpower in the Making. London: HarperCollins

Keohane, R. O. (1984). After hegemony: Cooperation and discord in the world political economy. Princeton, NJ: Princeton University Press.

Keohane, R. O., & Nye, J. S. (2001). Power and interdependence (3rd ed.). New York: Longman

Kiggins, R. D. (2011). Wired world: US policy and the open door internet, Dissertation, University

Koh, HH. (2012). International law in cyberspace. Remarks at USCYBERCOM Interagency Legal conference. Ft. Meade, MD. Retrieved September 18. 2012. from http://www.state.gov/s/l/releases/remarks/197924.htm.

Kohara, M. (2005). Information power and International Security. Progress in Informatics. No1.

Libicki, Martin C. (2007). Conquest in Cyberspace: National Security and Information Warfare. London: Cambridge University Press.

Nye, Joseph. (2002). The Paradox of American Power: Why the World's Only Superpower Can't Go It Alone. Oxford: Oxford University Press.

Nye, Joseph. (2011). The Future of Power. Bulletin of the American Academy of Art Sciences. Spring. Vol. LXIV. Issue 3. pp. 45-52.

Rothkopf, D.J (1998). Cyberpolitik: The changing nature of power in the information age. Journal of International Affairs, 51, 325-360

Schjolber, S., & Ghernaouti-Helie, S. (2011). A global treaty on cybersecurity and cybercrime. (2nd ed.). http://www.cybercrimelaw.net/documents/A Global Treaty on Cybersecurity and Cybercrime, Second edition_2011.pdf

Sofaer, A. D. Clark, D, Diffie, W. (2010). Cybersecurity and international agreements in Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for U.S. Policy, Committee on Deterring Cyberattacks: Informing Strategies and Developing Options: National Research Council. Available:

https://download.nap.edu/catalog.php?record id=12997.

Spade, J. M. (2012). Information is power: China's cyber power and America's national security. Carlisle Barracks, PA, US Army War College

Sternstein, A. (2011). International cybersecurity treaty might not be achievable, Report says. Available via Nextgov.

Sternstein. A. (2012). U.S., Russia, other nations near agreement on cyber early warning pact. Available via Nextgov. http://www.nextgov.com/cybersecurity/2012/12/us-russia-other-nations-near