CONCEPTUALIZATION OF SYMBOLIC SECURITY STRATEGIES OF AMERICAN CYBER DIPLOMACY

Hazhir Azarshab[1], Reza_Majdi*[2]
[1.] PhD Student of International Relations, department of law and poitical science, University of Tehran, Tehran
hazhirazarshab2020@gmail.com
[2.]PhD Student of International Relations, department of law and poitical science, University of Tehran, Tehran(Responsible)
Reza_majdi@outlook.com
ORCID:0009_0007_2074_1067

Abstract
America's main cyber policies, as the fourth pillar of democracy, have a significant impact on the domestic and foreign policy of this country. On the other hand, nowadays, the cyber space has become one of the most important aspects of security, so that with the growth and development of cyber technology, we see an increase in risks in this field. Different actors, both governmental and non-governmental, have emerged in this field, and each of them has taken actions against American national security in a way and based on their goals. In the meantime, although America is considered as the main developer of cyber space, it is a leading country in this field. The comprehensive development of the Internet and the excessive dependence of this government's sensitive infrastructure on information technology have exposed it to a variety of cyber threats. The banking network and Malaya to public services, civil and military networks are all dependent on the network. In case of cyber disruption, all of them will stop working. By examining the cyber incidents from the era of the previous presidents of the United States to the present day, the stages of the cyber threat in the order The political and then security work of the American government in details of the logical process that went through so that cyber security rose from a marginal issue under the general title of sensitive infrastructure to the top of American security threats. In this article, with the aim of identifying the components of cyber diplomacy in the United States of America, An attempt is made to analyze and examine the dimensions and frameworks of American diplomacy in the field of national security, as an indicator and example of the current national affairs of this country from the conceptual aspect of cyber diplomacy's symbolic security strategies.

Keywords: strategy, diplomacy, cyber security, America

1. INTRODUCTION

Today, many countries in the field of developing advanced technologies have established strict laws and regulations to control cyber security crises, and America has implemented new strictures in this direction. Cyber security is a key challenge for governments, companies and users of the world. The number and damages caused by various types of cyber attacks have increased significantly in recent years along with the growth of technology. According to experts, the global cost of cyber attacks for stakeholders in this field will reach about 10.5 trillion dollars by 2025. (1) For this reason, many governments of the world, especially the US government, have come to the conclusion that cyber security should be one of their main priorities and focus areas. Today, many of the world's leading countries in the field of developing advanced technologies have adopted strict laws and regulations to control cyber security crises and reduce the damage of attacks in this field. (2) Experts consider the main challenge of this field to be the lack of a single global front responsible for ensuring cyber security. In such a situation, many judicial institutions around the world have been obliged by statesmen to establish laws in this area on a national scale. This can create a favorable environment for cybercriminals to take advantage of gaps in regulations. The statistical reports of the United States indicate that most of the losses caused by cyber attacks and intrusions into

Digitla's infrastructure are directed at the Malay sector. This sector is very vulnerable to cyber attacks and crimes; Because banks and public institutions have access to a huge amount of users' personal data. In addition, without appropriate measures and policies in place, a cyber security threat can cause chaos and collapse for institutions. This is why experts consider effective and efficient cyber regulations to be very important and vital for this field. (3) Although America is considered as the main developer of cyber space, it is a leading country in this field. The all-round development of the Internet and the excessive dependence of America's sensitive infrastructure on information technology have exposed it to all kinds of cyber threats. Banking and Malay network to public services, civil and military networks are all dependent on the network, in case of cyber disruption, they will all stop working (4). By examining the cyber incidents from the Clinton era to Trump, we discuss the stages of the cyber threat being raised in the political agenda and then the security agenda of the American government. Also, we examine in detail the logical process that cyber security went through to rise from a topic on the sidelines under the general heading of sensitive infrastructure to the top of America's security threats. The creation and role of the institutions involved in cyber security is observed during the process of securing the cyberspace in America. The decision-making structures of the White House and Congress do not have the same approach to cyber security of critical infrastructure. In this article, we will discuss the interaction of Congress and the White House in creating, expanding or limiting the agenda of American cyber institutions.

2. THEORETICAL FOUNDATIONS OF CYBER DIPLOMACY

To examine the tools of American cyber diplomacy, it can be used to take help from the theories of communication science as theoretical foundations and to identify the effective factors on increasing and decreasing the impact of various messages and demands on people. These factors act as involved variables and determine the intensity and weakness of the influence of Iranian cyberspace users. In this context, two theories about the interaction between the media and its audience and how the media influence the audience can be used.

A) Using Giddens' theory of construction, it is concluded that the higher the participation of users in American cyber diplomacy sites by commenting, sharing requests, etc., the more likely they are to be influenced, but the more passive the users are and the more non-participative they are, the more likely they are to be influenced. Lower. Because according to this theory, humans create structures, but they are influenced by them in the later stages, so the internet and internet sites are the product of the meaningful action of humans and have structures created by humans. But after this structure is formed, it imposes restrictions on its users (human factors). When dealing with the Internet, unlike other conventional media, people are not simply placed in the category of producer or consumer, but they can have these two roles at the same time and engage in production and reproduction, but when dealing with this structure, the amount They have different timeliness and participation. In fact, the more immediate and involved people are in facing the Internet, the more likely they are to be influenced. On the contrary, the less immediacy and participation people have in facing the Internet, the less likely they are to be influenced. (5)

b) Based on the theory of cultivation or cultivation, it can be concluded that the amount of use and the actual amount of perception and trust in the content of American cyber diplomacy sites are effective in influencing the users. In other words, with the increase in the usage and perception of these sites by Iranian cyberspace users, the probability of being influenced by them increases, and the less users are exposed to such content, the less likely they are to be influenced. Because according to this theory, frequent exposure to a certain media causes a change in attitude and creates views that agree with the content of the media in the audience. (6) However, for a better understanding of the functioning of cyber diplomacy and designing a theoretical framework in this field, the actor-network theory can be used. This theory has been adopted by French researchers and John Law since the mid-80s based on the works of Bruno Latour and Michel Claven. This theory is a conceptual framework for examining social-technical collective processes of the British anthropologist, in which there are both technical and social scientific aspects, and it helps to understand social movements and current affairs based on science and technology networks. . (7)

One of the advantages of this theory, which helps to understand cyber diplomacy, is that based on it, there is no fundamental difference between the scientific current and other social currents, and therefore, the mentioned theory has a mixed view of the production of science. In other words, this theory avoids one-sided approaches of realism (emphasis only on natural and real things) and social constructionism (purely cultural narration of things and definition of nature in the framework of cultural contexts) and emphasizes that science is a heterogeneous engineering process that The production of those social, technical, engineering and textual factors and components are intermingled or put together and finally transformed or translated and understood. (8) With the emphasis of this theory on the integration of social sciences and technology, demarcation between society and nature, right and wrong, human and non-human, text and content, agency and structure, micro level and macro level phenomena, theory and data, data and Application, engineering and sociology issues are rejected and the formation of nature and society, subjectivity and structure, reality and fantasy are considered to be caused by collective and networked immediacy. (9) Actor in this theory means non-human entities including machines, texts and a combination of them. Activists are a combination of objects, identities, relationships and rules that these categories are symbolically assigned to them and are able to break into other heterogeneous networks, either individual or collective, or build a nest in them. Also, the current or independent agent is an agent who can be connected with other agents or act separately. Active actors enter network associations, which in turn define and name them and give them meaning, movement, purpose and effectiveness. On the other hand, they gain their identity from them. In other words, networks allow the active actors to define and specify their essence, intention, action and mentality, but these active actors in the process of scientific work have turned into a network and are called They develop a network and find a network identity. They do not have a specific foundation or prior essence and nature, and their nature results from networks. (10) The important result of accepting this theory in the field of social sciences is that social life is built by other networks and none of these two can exist without the other. It cannot be reduced to purely human or non-human factors and the presentation of explanatory models In the field of social sciences, it is reductionist based on only one human or non-human factor. Society is a set of heterogeneous social networks consisting of human and non-human factors such as space, objects, etc. (11). "social matter" is the interaction of social and technological worlds and these two are nested in each other, are inseparable and are constantly in each other's solutions. Also, the ability of humans to develop social networks is not only due to their interaction with agents of the same type or other humans, but also due to interaction with heterogeneous and non-human agents (12). If we want to connect this theory with our discussions about cyber diplomacy, we can say that the current actors are government agents (diplomats), individuals and organizations, and the actor is the Internet and its subsets. Therefore, here we are facing a heterogeneous and inconsistent network that has human and non-human components. The non-human and technological components are various software and hardware, and the human and social components are the people who designed, built and installed these software and hardware, as well as the groups, organizations and private and non-governmental institutions that use From these networks, they cause their life to continue. And especially to explain how the mentioned theory is a reflection of international relations in the field of information technology and the widespread use of the Internet by diplomats and diplomatic institutions and all kinds of digital tools, including computers, mobile phones, various programs and software in the hook of a network. Heterogeneous can be used to achieve foreign policy goals and secure national interests in the international arena. All these hardware, software, diplomats, regular internet users, diplomatic government institutions, international organizations, etc., as actors and active actors, create a systematic network that continues in the internet and cyber space for the time being. to give In the cyberspace, the emergence of disruptive technologies such as cloud computing, Internet of Things, big data, quantum computing, cognitive science, and cyber physical systems is the foundation for creating a fundamental transformation in the fourth industrial revolution. The defense and military fields have undergone fundamental changes under the influence of these new technologies and are forced to adapt to this phenomenon. The change in the nature of war and turning to cyber equipment and weapons has become an alternative to nuclear weapons, and this issue plays an important role in national security and international interactions. However, the development of new technologies in the cyber space brings various threats and risks, the greater the dependence on this space, the greater the depth and impact of the risks caused by these threats (13). In the fields of defense and military, each of the technological macro-trends of the cyber space brings challenges and threats that the need to face them smartly is necessary and inevitable. In this section, some applications and cyber threats of these technologies are summarized in Table (1).

Table (1): applications and threats of emerging cyber technologies in military and defense systems (7,8,13,14)

	Military applications	**Cyber threats**
Internet of Things	In the military field, Internet of Things is used to guide and manage equipment, supplies, military affairs, soldiers, etc., on the battlefield, missions and trainings, for example, to inform commanders about the physical health status of troops at any time and to facilitate decision-making in difficult moments. In the aviation industry, it is used to use pressure, temperature, vibration, etc. sensors and send them to the pilot and control tower.	The use of Internet of Things in military equipment increases the possibility of espionage, penetration and theft of information. Also, if cyber security mechanisms are not used, the possibility of using cyber weapons to damage equipment and forces increases..
cloud computing	In defense organizations, information and communication technology has been considered in order to create reliability, flexibility, empowerment, economy, ease and speed in providing services, reducing the cost of support operations and integrating communications. In addition, in these organizations, the efficiency, effectiveness and agility of the mission implementation process are important demands that encourage these organizations to use cloud computing..	In defense systems, even if using a private cloud physical platform, sending, receiving and storing data in an infrastructure that is out of scope and control; It faces security challenges such as confidentiality, authentication and access control. In addition, in defense systems, information sharing requires interfaces to adapt to the cloud infrastructure, and the security of these interfaces is also problematic..
big data	In defense and security organizations, we are faced with big data in order to know the situation of the organization and forces, make strategic decisions and carry out military operations. This massive amount of data may be machine-made and obtained from various equipment such as ships, aircraft and vehicles, satellites, drones and surveillance radars, tracking aircraft, wireless smart sensors on the battlefield; Or it has human origin and it is generated from social media, websites, social	The variety of collected data and the need for processing and analysis speed determine the necessity of using big data technologies in modern systems. In defense and security organizations, due to the development and expansion of various communication systems, data sources and data volumes are increasing exponentially. Collecting and extracting information from this massive data requires the use of new big data technologies. But in case of technological dependence, it will create cyber threats. In big data, due to the large storage volume and high processing power, extracting

	networks, transactions, etc. In defense systems, data is obtained from environmental sensors, satellites, electronic warfare systems, Linet, Comint, Sigint, social media, etc. This information is collected in an Enterprise Data Hub (EDH) for the purpose of enrichment, correlation discovery, sharing and updating, and after advanced and real-time analysis, it is used to create warning and awareness or to assess the battlefield.	knowledge from data involves various steps such as receiving, storing, transferring, managing, analyzing and illustrating data. The accumulation and maintenance of this data will bring threats such as information leakage and cyber espionage. Deciding how to manage the battlefield and dominate the battlefield in the future requires the use of big data and related technologies. However, there is always the possibility of distorting and changing information and making a wrong decision, or receiving fake orders. The sensitivity and importance of information in defense systems requires the acquisition of advanced encryption technologies, and if cyber security is not guaranteed, data centers are exposed to cyber attacks and threats.
Physical, cyber systems	An efficient military organization must be flexible, responsive, innovative, resilient and adaptable in today's network-centric warfare. These features are performed by simultaneous and automatic systems. The main challenge of these systems is the integration of different physical, cyber, information and cognitive domains. The solution to this problem is to use physical and cyber systems. In physical cyber systems, interaction between mental elements and physical elements is established in an effective control chain. The integration of physical systems, information sharing, decision-making processes and the process of synchronizing operations in such organizations will make them more dynamic than traditional systems. The use of physical cyber systems in defense organizations causes, instead of controlling individual actions, the synchronization of information is done through recognition and integrated decision-making in guiding organizational behavior, and instead of an individual or regional organization, a multilateral and all-purpose organization is created.	Creating a favorable image of joint operations and clarifying missions, based on the architecture of cyber-physical systems, requires integration between the resources of physical and human domains. Cyber security challenges can be threatening if human factors are not understood and the equipment is not indigenous. In physical cyber systems, information sharing and the matching of information and knowledge are done through the infrastructure of cyber space. This issue requires the allocation of an independent and secure infrastructure to prevent cyber attacks by cyber criminals and hostile groups. Synchronization and mission synchronization among operational units is one of the important challenges that will be the source of many threats in physical cyber systems based on the global Internet network..

3- Dos and don'ts of cyber diplomacy

The use of diplomatic tools and mentality in order to promote the governance of the virtual space of countries is cyber diplomacy. Just as the virtual space has affected all areas of human life, international relations is also one of the most important evolved fields. Different countries have resorted to the use of cyber diplomacy strategies and use it both negatively and control cyberspace threats and positively and develop and export their cyberspace services and content. Considering its special situation, such as conflicts with issues such as sanctions or the challenge of interacting with technology giants, or the country's civilizational view in exporting services and cyberspace content, Iran should have a special look at cyber diplomacy. For example, in the seventh paragraph of the general policies of computer information networks in 1377, it is stated: "Appropriate measures to achieve international covenants and regulations and to create information unions with other countries, especially Islamic countries, in order to create a balance in the field of international information and to preserve and protect the identity and National culture and confronting global domination" also in paragraphs 3, 4, 19 and 22 of the goals of the strategic document of the Islamic Republic of Iran approved by the Supreme Council of Cyberspace in 1401 on "achieving the power of the country's cyberspace at the global level and the first place among the countries Region", "Ensuring rights, security and national interests in cyberspace and realizing multilateralism in internet governance", "Achieving a superior position in the value chain of services and content in the countries of the region and the Islamic world" and "Transforming the country's cyberspace into a regional center of exchange Data and provision of communication and informational and commercial infrastructure services to the countries of the region" has been emphasized. Using the capacity of regional and international assemblies and organizations requires a detailed record and counting of its positive and negative consequences. The Internet Governance Forum (IGF) is an event and forum to discuss and present ideas about Internet governance and its issues and challenges. Assemblies such as IGF, WSIS and some other events have been a response to American unilateralism in internet governance. Also, due to its conversational nature, this forum is less official than other organizations such as ITU or ICANN, and to some extent it can be said that it does not have binding obligations. From this point of view, it seems to be the right place for the starting point of cyber diplomacy along with some other advantageous points such as ECO, Shanghai cooperation, BRICS. In this event, due to the closeness of IGF2023, the history, future prospects of this forum and the requirements and duties of Iran's role in this event have been discussed. In the domain of cyberspace governance, we are facing self-regulation and monopolization of the Internet by a company in order to secure the interests of America. In recent years, the use of multi-stakeholder terms and the creation of circles such as the Information Society Summit or the Internet Governance Forum have emerged as a safety valve to adjust the atmosphere of Internet exclusivity (18). From the point of view of the book Cyber Diplomacy towards Iran from 2006 to 2012, which was published in 1402 by Reza Magdi, it is argued that, in a realistic view, technical-legal arrangements are necessary and the introduction of powerful cyber diplomacy in order to influence the governance of cyber space, which is currently Present in our country, it is given less attention. In addition to paying attention to assemblies such as the Internet Governance Assembly, the capacity of organizations such as ECO, BRICS, etc. should also be used. Also, the use of non-governmental institutions and think tanks to produce innovative discourse in this direction is very important. In the field of cyber diplomacy and experiences in the world, it can be said that today, different countries are taking many measures in order to use cyber diplomacy. Participation in the Convention on Cyber Crimes, the Symposium of Regulators of the World Telecommunication Union and the meeting of the presidents of the countries with the CEOs of large technology companies are among the examples in this field. In this issue, we also see the discourse confrontation between the two countries, the United States and China. In such a way that the United States of America seeks to build a coalition by using the literature of the fragmentation of the Internet, and in contrast to that, China has created a discourse against the United States by holding the World Internet Governance Summit of China with the slogan of a unified Internet and respect for national laws. There is no doubt about the need to play an active role in international forums, what is important is the value of each of these forums. At the very least, such assemblies have led to the presentation of ideas, which is a positive thing, and in this field, the capacities of universities, non-governmental organizations and the private sector of the country should be activated. Issues such as protecting the rights of Iranian users in social networks, cyber security, and the development and export capacities of native cyberspace services are among the issues that can be raised by Iranian participants in these forums (19). Today, governance arrangements have changed and technical issues of the Internet have become pressure tools in legal, economic and political fields. At first glance, the model proposed by these associations with multi-stakeholder literature seems to be a desirable model. In this model, redistribution of authority occurs and governments share a greater share of authority with other actors (20). In such a situation, international law is evolving. We have three main scenarios in front of us in this field. First, let's leave ourselves in the hands of fate and dissolve in the existing world governance. Second, we should establish a national governance with a monopoly in our own fortress, regardless of global governance, and third, we should build alliances with other countries in existing advantageous points. The current problem of our country is non-participation in international forums. There is no doubt about participation in the Internet governance forum, but we should focus on some areas to create an effective and targeted coalition. The countries that we have recently joined can create a good opportunity in this field (16). Participation in international forums can be a strategy in the direction of national branding and improving the image of countries in the field of cyberspace governance. Currently, there is no good picture of Iran's cyber space governance in the world (13). In the last decade, there is a new arrangement in the global governance of virtual space. Iran should establish its position in this new arrangement by forming alliances with emerging countries in this arena. The requirement to channel this new power is to present an effective show. Iran has new words in various fields of virtual space, which should bring this speech into the arena of dialogue by participating in international forums. Such an atmosphere will lead to the formation of a new discourse and ultimately create strength for the country. If we wander into the realm of fruitless drama reading, we have only helped to reinforce America's unipolar rule in cyberspace. The Internet Governance Forum can be a good starting point for testing the country's participation in international forums in the field of virtual space. Presenting an intelligent show and seizing the opportunity to talk should be on the political agenda of the country (19). There are two types of power. Soft power deals with imagery and hard power promotes governance by involving interests and needs. Cyber diplomacy is very dependent on your power. The Internet is one of the tools that fulfills the needs, but the question is who dominates the Internet. The Internet Governance Council will not have any results for us in terms of hard power and we can only use it to advance our soft power (20). Nowadays, technology companies play a significant role in cyber diplomacy, so in order to adopt a strong cyber diplomacy and create our discourse, we must move towards the globalization of the country's platforms. The creation of large technology companies in order to challenge the current state of global Internet governance and increase the country's strategic depth, considering the capacity of Persian-speaking countries and neighboring countries, should be on the country's agenda. Also, by using the academic and research capacity of the country, we should produce and promote a new discourse (19).

4. BASICS OF THE UNITED STATES CYBER STRATEGY DOCUMENT

The emergence of the Renaissance in the 15th century led to the emergence of an important cultural movement that carried the chains of the scientific revolution, religious reforms and artistic developments in Europe. The Age of Enlightenment in the 17th and 18th centuries of Europe also carried the main message of modernity, which actually explained and developed the ideas that emerged from the Renaissance. As a result, although we cannot talk about causal relationships, the Enlightenment was the foundation of an intellectual-philosophical movement in the history of Western thought, which brought about huge revolutions in the field of science and philosophy and ultimately caused the complete disappearance of the medieval worldview. According to the above-mentioned tremendous developments, in 1688 AD. The English revolution came to fruition and the parliament of this country succeeded in turning the country's political system into a constitutional monarchy. Later and in 1776 AD. The American colonies, which were loyal to Britain for a long time, declared their independence from this country and considered the tax policies that the British imposed on them to be a violation of their natural rights. The result of the American

Revolution was the writing and approval of the United States Constitution in 1787. The United States Bill of Rights was quickly ratified in 1789 and granted its citizens certain natural rights based on liberal ideals. When, theoretically, the globalization of trade is considered as a guarantee of peace, it is obvious that the dominance of global trade platforms and their control is also a matter of competition; This shows the importance of the seas and the legislation of this area during the past centuries and tells us why the superpower of those days, England, had a powerful shipping, had a dual approach to the security of the seas, and while dealing with annoying pirates, to advance its intentions. It uses them against its competitors and why this country is still the most important provider of marine insurance services in the world. Despite Kant's theory, until before the Second World War, we witnessed a very slow change and the relative continuity of what is called the so-called European balance. And only when Hitler's non-commitment to the balance of Europe divided the European countries into two categories, allies and allies, and brought many destructions, the idea of the balance of Europe was fundamentally left out of the agenda, and the idea of eternal peace, the foreign policy of the United States. and formed its partners, that is, European countries. According to Polanyi, as soon as the world economy, which was the mainstay of the balance of the international system, collapsed, it was no longer possible to guarantee peace. In such a situation, the United States of America, which was spared from the ravages of war, paid attention to Kant's idea of eternal peace. America's idea of establishing and renewing peace in war-torn Europe was a mechanism of mutual enrichment. (14). They believed that as in the abstraction of the individual level, through the exchange in the free market system, the maximum profit for the seller and the minimum cost for the buyer emerges, the free market system should also prevail at the global level so that the benefits are distributed fairly among the countries. According to this argument: the idea of European progress is a fundamental theme in liberalism and it completely changes the themes of European balance... In order for the freedom of the market to guarantee the mutual, interconnected and more or less simultaneous wealth of all European countries... an excellent market is necessary. Wide and even if it were possible, everything in the world that can be put on the market, would be gathered around Europe and for Europe. In other words, when it was established as a rule and goal that the enrichment of Europe should be achieved in a collective and unlimited way, not in the form of one becoming rich and others becoming poor, we have been called to a globalization of the market. The whole world should gather around Europe to exchange European products and themselves in the European market... Now, the opening of a world market... makes it possible to avoid the conflicts caused by a limited market. But the release of this global economic game requires the difference between Europe and the rest of the world in terms of quality and dignity. In other words, on the one hand, we have Europe and Europeans as actors, and on the other hand, it will be the world. The game is played in Europe, but the share of the game is the world. After two centuries, today and in the age of communication revolution, Kant's concept of cosmopolitan society has found an objective and tangible meaning in the hook of the doctrine of civil society (15). Therefore, the national and economic security of the United States of America depends on the safe operation of critical infrastructure. Cyber security threats arise from the increasing connectivity and complexity of critical infrastructure systems and endanger national security, public health and safety. Like financial and reputation risks, cyber security risks will also affect the survival of companies. Cyber security threats can drive up costs and reduce revenue. Cyber security threats can damage companies' ability to innovate, acquire and retain their customers. (14)

To address these risks, the President of the United States issued Executive Order 13636 "Improving the Security of Critical Infrastructure" on February 12, 2013, which determined that "It is the policy of the United States to improve the security and resilience of the nation's critical infrastructure, the efficiency, innovation, and financial success of the environment." It preserves cyberspace and promotes safety, security, business confidentiality, privacy, and civil rights." In enacting these policies, the executive order seeks to develop a voluntary risk-based cybersecurity framework—a set of industry standards and best practices that will help organizations manage security risks. The resulting framework was created from the interaction between the government and the private sector and uses a common language to address and manage cyber security risks in a cost-effective manner based on business needs and without imposing additional regulatory requirements on businesses. The framework focuses on using business drivers to drive cybersecurity activities and considering cybersecurity risks as part of an organization's risk management process. The framework consists of three parts: framework core, framework profile and framework implementation layers. The core of the framework is a collection of cybersecurity activities, outputs, and informative references that are common across infrastructure sectors and provide descriptive guidance for the development of individual organizational profiles. Through the use of profiles, the framework will help organizations align their cybersecurity activities with their business, fault tolerance, and resource requirements. The layers create mechanisms for the organization to observe and understand the characteristics of its approach to cyber security risk management (12). The executive order also requires that the framework include methodologies to protect individual privacy and civil rights when large organizations with critical infrastructure conduct cybersecurity activities. As current processes and needs change, the framework helps organizations consider privacy and civil liberties as part of a comprehensive cybersecurity program. The framework enables organizations—regardless of size, cyber risk level, or cybersecurity sophistication—to apply risk management principles and best practices to improve the security and resilience of critical infrastructure. Related to today's multiple approaches to cybersecurity, the Framework gives structure and organization to these fragmented standards by bringing together standards, guidelines, and practices that work well in today's industry. In addition, since the Cybersecurity Framework references the world's recognized cybersecurity standards, the framework can also be used by organizations located outside the United States and serve as a model for international cooperation in strengthening critical infrastructure. (14) The framework is not a one-size-fits-all approach to managing all aspects of critical infrastructure. Organizations will have unique risks—different threats, different vulnerabilities, and different fault tolerances—and how to implement measures within the framework will vary. Organizations can identify activities that are critical to delivering critical services and prioritize investments to maximize the impact of every dollar they spend. Finally, the framework seeks to reduce and manage cyber security risks. The document framework is live and will be updated according to industry feedback. As the framework is put into practice, lessons learned will be incorporated into future versions. This ensures that the cyber security framework meets the needs of operators and owners of critical infrastructures in the challenging environment of new strategies, threats and risks (15). According to what has been said, it can be claimed about the National Cyber Strategy document of the United States of America:

- The meaning of freedom in this document is only the independence of citizens against the government, and what guarantees the provision of human rights - in a fair and not equal way - is competition in the conditions of freedom.
- The document defends civil liberties, limited government, private property and emphasis on the free market
- In this document, the collective interest that is realized through the freedom of the market forms the basis of everything, including society, culture and politics.
- Due to the predominance of the idea of a minimal government in this document, providing security and facilitating trade - in the international space - is the most important task of the government, and for this reason, the government has no plans to take over this field - at the national level.
- Jurisdiction, meaning the creation of an international legal system, as well as international rights to exploit the virtual space - as an emerging market - is mentioned in the document.
- According to the document, the globalization of business in the virtual space - as an environment of free competition - will be a guarantee of world peace
- While fighting and confronting any sabotage and threat to the security of its cyberspace, the United States will not fail to take any action to threaten its competitors and enemies, including the creation of various types of malware, espionage systems, and abuse of cyberspace.

- The liberal rights stated in the American Declaration of Independence include: life, liberty and the pursuit of prosperity and happiness constitute the pillars of the document.
- The values of the document are consistent with the goals and slogans of the American Revolution, which are stated in the Constitution and the Bill of Rights of the United States
- Although according to the commitments of the United States to its European allies after the Second World War, which led to the formation of international institutions, the United States is supposed to ensure the mutual, interrelated and more or less simultaneous wealth of all European countries, but it seems that today the United States has fundamental doubts. He adheres to his previous commitments, and for this reason, on the one hand, he is trying to globalize the virtual space market, and on the other hand, he does not have a plan to share his former partners in this market, or at least he believes that his dignity and rank in this market is completely different from others. Is.
- Since the "National Cyber Strategy Document of the United States of America" has a direct relationship with the cultural-historical context and economic-political structure of that society, it is likely that the success of the document's implementation will be accompanied by public participation and greater ease.
- Finally, if we know that the United States considers cyber space as the basis of today and tomorrow's world trade and as a result of world peace, we will clearly understand the place in the improvement of cyber space in recent years. In order to examine the document from this point of view, we will have an overview of its various parts.
- One of the characteristics of the document is the appropriateness of the tone with the audience, which begins with this phrase:

"My American companions; My top priorities are protecting America's national security and enhancing the well-being of the American people. Ensuring the security of the cyber space is necessary to achieve these two goals. Cyberspace is an inseparable part of American life today, including our economy and defense sector.

The other part of the document entitled "How did we get here?" is related to the necessity of writing such a document in which the political position of America in cyberspace is clarified. Some of the key phrases in this section are as follows:

- The emergence of the Internet and the increasing centrality of virtual space in all aspects of the modern world was related to the emergence of America as the world's only superpower.
- In the last quarter of a century, the initiative and intelligence of the American people caused the growth and evolution of the cyber space, and on the other hand, the cyber space has become the basic foundation for the production of wealth and innovations.
- Americans sometimes admit that the United States will remain the dominant power in cyberspace without any problems.
- Americans believed that the expansion of the Internet would lead to the realization of universal ideals of freedom of speech and individual social freedoms all over the world.
- Americans believed that the Internet would provide opportunities for expanding communication, commerce, and the free exchange of ideas.
- Much of the world has embraced America's vision of an open and shared cyberspace that benefits both parties.
- Our competitors and opponents... even though they use the open internet, they limit their people's access to this space and control their access, and for now, they are weakening the principles of an open internet in global circles. While participating in destructive economic espionage operations and conducting hostile cyber activities, they disrespectfully violate the laws of other countries, cause many economic problems, and harm individuals, commercial and non-commercial interests, and governments around the world.
- They [competitors and adversaries] see cyber space, where America and its friends and partners are vulnerable, as an arena to neutralize the military, economic and political power of the United States.

- Russia, Iran, and Korea have fearlessly carried out various cyber attacks to harm the business of the United States and the world, our allies and partners, and have not paid any compensation that can prevent cyber attacks in the future. China engaged in an internet economic espionage operation and stole trillions of dollars of our intellectual achievements. At present, non-state actors, such as terrorists and criminals, have used cyber space to gain profits, recruit new forces, advertise and attack against the United States of America and its allies and partners, and most of their movements are supported by enemy governments.

Finally, the document presents four principles: first (protecting the American people, homeland and American way of life, second) increasing American prosperity, third (maintaining peace alongside power, fourth) promoting American influence.

5. STATE OF CYBERSECURITY REGULATION IN THE UNITED STATES

- Cybersecurity regulation in the United States

Generally, there is a federal cybersecurity law in the United States of America. Meanwhile, some states of this country have also passed their own regional laws to ensure cyber security.

- Gramm-Leach Bliley Act (1999)

This measure is the first cyber security measure for Malay institutions in the United States. According to the text of this law, banks, credit unions, and other regulated institutions must establish, implement, and maintain data security throughout their tenure process.

It is enforced by the US Federal Trade Commission and, at a basic level, requires institutions to inform customers about the data they collect and allow them to opt out.

In addition, the teams responsible for assessing the compliance of organizations and institutions with these rules must develop their own programs to demonstrate the safety of physical, administrative and technical data. In this regard, organizations and institutions under supervision are required to comply with the following rules:

- They should declare the nature of their current situation.
- Supervised entities must make their current scope clear and obvious.
- Identify the potential risk of their current affairs for their customers.

The aforementioned law is considered one of the oldest legal measures in order to determine cyber security standards for organizations for the time being. Nevertheless, the legislative environment in this field is considered one of the most dynamic parts of the United States judicial system, and the legislators of this country are always trying to update the rules according to the requirements of this field.

- Cyber security requirements for devices connected to the Internet

The Biden administration has recently developed the Internet of Things (IoT) cybersecurity labeling program aimed at protecting American citizens from the myriad security risks associated with Internet-connected devices. The said program, named "U.S. Cyber Trust Mark" helps American citizens in the field of purchasing devices connected to the Internet that are safe and resistant to cyber attacks. Among the requirements of this new mandatory standard, set by the US National Institute of Standards and Technology (NIST), are that devices have unique and strong default passwords, protect stored and transmitted data, provide regular security updates, and have Incident detection capability pointed out.

- The cooperation of numerous supervisory bodies for security monitoring of specialized departments

In addition to the laws in the federal judicial structure of this country, many organizations in this country are also responsible for dealing with matters related to the protection of cyber security and reducing cases of user data breaches. Senior cyber security officials of the United States always emphasize the issue of sharing information in order to protect the internal networks of this country against hacker attacks. According to the data published in this case, the sharing of information between the Cyber Command (U.S. Cyber Command) and the Cyber Security and Infrastructure Organization of the Department of Homeland Security (CISA) has in many cases neutralized malicious cyber attacks on the American elections. Cyber commanders in the Ministry of Defense of this country and the US Federal Civilian Cyber Security Agency always claim that the relationship between these two organizations is necessary to defend this country against foreign hackers. Eric Goldstein, the executive assistant of the Cybersecurity and Infrastructure Organization of the US Department of Homeland Security, recently made a comment on the sidelines of the "RSA2023" summit on this matter, claiming that the private sector does not find information sharing very useful and believes that it leads to providing effective guidance in This is not the case; However, despite the lack of success in realizing information cooperation between the public and private sectors, the exchange of information between the Cyber Security and Infrastructure Organization of the United States and the Cyber Command of this country has been fruitful.

- **Regular publication of cyber security strategy on a national scale**

Compilation and publication of the cyber security strategy document is another tool at the disposal of American politicians in order to increase cyber security and prevent attacks in this area. On March 2 this year, the White House published the latest version of the country's cyber security strategy. The mentioned document is considered as a way to increase the protection of different parts of this country against the ever-increasing cyber threats. The latest strategy emphasizes stricter regulations to ensure cybersecurity for industries and improve cooperation between the government and the private sector. In this strategy, China and Russia are mentioned as the most important cyber security threats to the United States, and according to experts, one of its goals is to curb Russia's cyber power. This strategy also emphasizes improving some standards in computer systems and requiring cloud companies to verify the identity of their foreign customers.

- **The axes of America's 2023 cyber security strategy**

The framework of the recent cyber security strategy of the United States, which was compiled and published by the Biden administration, focuses on several key axes, some of its headings are as follows:

- Defense of the critical infrastructure of the United States
- Disruption and action to confront and destroy external threats
- Orienting the market in order to improve cyber security indicators
- Strategic investment in order to increase resilience
- Increasing international participation in order to achieve common goals

- California Consumer Privacy Act and Colorado Privacy Act

Data privacy is a key aspect of cybersecurity protection. Along these lines, states such as California and Colorado have taken on data protection requirements by enacting their own data protection policies for businesses in their jurisdictions.

These policies are somewhat similar due to the great similarity of many data breach and cyber security risks and focus on actions and requirements that data controllers and processors can take to keep customers safe. The main purpose of these regulations is to give customers the right to opt out of data collection and to prevent their information from being transferred to third parties.

Managing cyber security risks to increase the security and stability of America's information and information systems.

- **Security of federal networks and information**

The responsibility for the security of federal networks - including federal information systems and national security systems - rests entirely with the federal government. In order to secure the federal information systems, the government will define the relevant authorities, obligations and responsibilities within and between the ministries and agencies in addition to establishing standards for managing cyber security risks. As part of this process, the administration will centralize some authority within the federal government, expand international agency oversight, improve federal supply chain management, and strengthen the security of US government contracting systems.

- **Prioritization of actions**

More centralized management and oversight of the federal government's civilian cybersecurity to secure the networks of federal agencies and departments, with the exception of national security systems and the Department of Defense (DOD1) as well as Intelligence Committee (IC) systems.), will do. This includes ensuring that DHS has full access to the agency's information systems for cyber security purposes and the ability to take appropriate and direct actions to protect these systems from various threats. Under the supervision of OMB, the administration is prioritizing work done related to Executive Order 13800 to transition agencies to shared services and infrastructure. DHS will also closely monitor these services and infrastructure in order to improve the cyber security situation of the United States. We will continue to develop centralized capabilities, tools, and services through DHS that effectively improve oversight and are consistent with applicable laws, policies, standards, and guidelines. It seems that in order to realize this, new laws and architectures are needed, which enable the government to make better use of the achievements. DOD and IC will consider these actions as actions that adequately improve the security of national security systems, DOD systems, and IC systems.

- **Alignment of risk management and current information technology**

Executive Order 13833, on improving the efficiency of the agency's chief information officers, strengthens the chief information officers (CIO) to achieve a higher level of efficient technology to carry out the agency's missions, reduce duplication of work and make information technology more effective. Department and agency leaders will empower and support their trusted CIOs to align cybersecurity risk management decisions with IT funding and procurement decisions. The administration, through OMB and DHS, will continue to lead and guide risk management initiatives in federal civilian departments and agencies, and CIOs will continue to play a proactive leadership role and ensure that IT procurement decisions are properly prioritized to secure data and networks. And, they will get more power.

- **Improving federal supply chain risk management**

The US government wants to integrate supply chain risk management with agency procurement and risk management process. This work is in line with federal needs to further ensure the security and reliability of technologies employed by the federal government, and includes better information sharing between departments and agencies to increase awareness of supply chain threats and repeat supply chain operations in government. United States, including the establishment of a chain risk assessment sharing service. It also includes finding deficiencies in the federally implemented system, such as creating more powers to eliminate intermediaries, regulated products and services. These measures will be synchronized with supply chain risk management measures in the national infrastructure.

- **Strengthening the cyber security of federal contractors**

The United States cannot afford to ignore sensitive government information or systems that are inadequately secured by contractors. Contractors perform important services for the United States government, and the systems they service must be properly secured. In the future, the federal government will be able to measure the security of its data by reviewing contractors' risk management practices and performing appropriate tests, trials, and responses of contractors' systems to incidents. Contracts with federal ministries and agencies will be designed to adopt measures aimed at improving cyber security. In the meantime, one of the concerns raised are the contractors who are responsible for the research and development of key systems used by the DOD in defense industrial centers. In addition, as recommended in the Executive Order 13800 report to the President on Modernizing Federal Information Technology, the administration will support the adoption of integrated deployment strategies to improve cybersecurity and reduce significant costs associated with the use of conflicting contract provisions across the federal government. . Measures will also be taken to ensure that federal contractors can receive and use shareable information related to vulnerabilities and threats when necessary.

- **Ensuring the leadership of the government in the best and most innovative way**

1- The American federal government ensures that the systems under its supervision and administration are in accordance with the standards and in the best state of cyber security recommended by the industry. Projects that receive federal funding must also follow these standards. The federal government uses its purchasing power to improve the performance of various sectors in products and services. Also, the federal government will be the leader in the development and implementation of standards in the best way, even in new and emerging areas.

For example, public key cryptography is essential to the secure operation of our critical infrastructure. To protect against the potential threat posed by quantum computers' ability to break public-key cryptography, the Department of Defense will continue to search, evaluate, and standardize quantum-resistant public-key cryptography algorithms through the National Institute of Standards and Technology (NIST). The United States will lead the way in protected communications by supporting the rapid adoption of NIST standards in government infrastructure and by encouraging people to do so.

2-Safe critical infrastructures The responsibility of securing national critical infrastructures and managing cybersecurity risk is shared between the private sector and the federal government. In collaboration with the private sector, we will use a cumulative risk management approach to reduce damage and increase the cyber security of critical infrastructure. At the same time, we use result-oriented methods to reduce the actions of our highly advanced adversaries that can cause large-scale or long-term destruction of critical infrastructure. It also deters enemy cyber activists by imposing costs on them and their sponsors using various means that are not only limited to legal prosecution and economic sanctions.

6. PRIORITIZING ACTIONS

- **Reconstruction of roles and responsibilities**

The US government clarifies the roles and responsibilities of federal agencies and expectations from the private sector in relation to cyber security risk management and incident response. This transparency will enable proactive risk management to identify threats, vulnerabilities and outcomes. It will also cause identification and communication of existing gaps between response actions during incidents and will increase routine training, exercises and coordination.

- **Prioritization of measures based on identified national risks**

The federal government will work with the private sector to manage risks related to critical infrastructure, which are most at risk. By identifying critical national functions, the government will achieve a comprehensive understanding of national risks, and by better managing these national risks, we will grow our cyberspace security proposals and partnerships. The government prioritizes measures to reduce risks in seven key areas: national security, energy and power, banking and public affairs, health and safety, communications, information technology and transportation.

- **Upgrading information and communication technology service providers as creators of cyber security**

Information and Communication Technology (ICT) is the foundation of every sector in America. ICT providers are in a special position to identify, prevent and mitigate risks before they harm their users. The federal government works with these providers to improve ICT security and resilience in a targeted and effective manner, as well as protect privacy and civil liberties. The US government will take steps to increase information sharing to empower ICT providers to respond to and remediate malicious cyber incidents at the network level. These measures will include sharing classified threat and vulnerability information with ICT operators and will also downgrade information to the unclassified level as much as possible. America promotes a secure, sustainable and flexible technology supply chain that protects security based on best practices and standards. The US government will bring stakeholders together to find solutions to challenges that arise at networks, devices and access layers. We will encourage industry certification organizations to ensure the effectiveness of solutions in the growing and threatened market.

- **American cultural diplomacy as a cyber power to deal with competitors**

During the Cold War, America has made the most effective use of cultural tools and information to destroy its rival, considering the importance of cultural diplomacy. However, in 1999, the US government dissolved this agency and integrated it into other sub-departments of the Ministry of Foreign Affairs, citing the end of the Cold War as the most important reason for this action. At the end of the 1990s, this agency had nearly 190 branches and offices in 140 countries and had a budget of 1.2 billion dollars. In addition to government institutions affiliated with the Ministry of

Foreign Affairs, many other strategic research centers and institutions have been established for this mission, of which the American "Culture and Art Center" is one of them. The announced goals of this center are presented in three sections as follows:

- Promoting public awareness of the importance of cultural diplomacy;
- Carrying out research projects in the field of cultural diplomacy;
- Practical opinion and direct influence on plans and budget allocation for the office of cultural and educational affairs in the US Department of State.

Americans believe that the revolutions that have started throughout the Middle East are a success for American foreign policy in the field of soft power in this region. In fact, the soft power that was created through the media and cultural diplomacy and exchange diplomacy has played an important role in creating the demands of the people who want democracy, human rights, and economic and social justice. But it should not be overlooked that the formation of popular uprisings in the Islamic and Arab world; America's hard power has been brought to its knees(17). Beside it, in America's cultural diplomacy, there are discourses, discursive procedures, social processes, and knowledge systems through which meaning is produced, recorded, analyzed, and transmitted(20).

Discourses as a comprehensive formative semantic analysis, processes create social procedures and relations, social identities, subjects and their capacities by giving them meaning (21). A discourse becomes dominant when a larger group of people and society accept the views hidden in it as a system of beliefs and common knowledge, and individuals and social actors obey and follow the meanings, concepts, values and norms in these discourses and systems of meanings. reproduces them. Following these components of the punitive power leads to self-discipline and self-regulation and reproduces that characteristic. Therefore, discourse procedures are considered one of the most important forms of soft power (18).

In the mid-1990s, after the collapse of the Soviet Union, the United States government felt unprecedented power and domination over the world, and saw no obstacle in the development of cyber infrastructure with private sector investment and management. But in the first decade of the 21st century (Bush era), when society and economy depended on this space, security concerns gradually emerged. Of course, cyber events such as hacking the traffic control system or a few popular websites were not something that shocked the society or the government of the United States (21). But what put the cyber issue on the political agenda of this era (Bush) was the atmosphere ruling the government due to the attacks of September 11, which caused the security aspects of all issues, even financial transfers above 10 thousand dollars, to come under the microscope. It was since 2009 that cyber evolution and the seriousness of terrorist groups in recruitment, advertising and communication; Also, the introduction of the offensive capabilities of cyber software led to the military-security use of this space. The chart below shows the change in conditions that led to the change in strategies. The first basic model in the field of cyber security is outsourcing to the private sector, which was first introduced in the second Clinton administration, and still, according to the law, some security institutions in America, such as the Department of Homeland Security, which deal with the private sector, are forced to act on that basis. do This model is developed based on the more effective functioning of the private sector and relies on the theory of gradual progress and the theory of self-management. The result of the security of cyber issues during George Bush's era was more government control over it and a change in the authority of security. These criticisms and efforts eventually led to the formation of a government theory of cyber security that considered private companies ineffective in providing cyber security to America's critical infrastructure. This theory, which was proposed by the warnings and recommendations of strategic think tanks of the United States at the end of the Bush Jr. period and was seriously pursued during the Obama period, did not enjoy full emergence and acceptance in all public and private circles until the end of the Obama period. Because this method, due to its problems and incompatibility with the American liberal system, faced with structural resistances, did not have much chance to fully emerge and underwent changes and transformations on the way to its approval in the Congress in 2012. The Obama administration wanted to use two economic and legal tools to encourage and punish companies engaged in cyberspace and sensitive infrastructure, but Congress never agreed to the second tool in a mandatory manner. Despite all these efforts, the White House still has not integrated its disparate cybersecurity agendas under a comprehensive strategy, as it has in other sectors. Of course, after the Russian cyber attacks in the presidential election, it seems that the position of the Congress is changing, but considering the result of the cyber scandals that ultimately led to the election of Trump, the Trump administration does not seem to have a plan to advance. have this strategy. It remains to be seen what will be the fate of the two-party plan that is being hammered out in the Congress in this regard between the White House and the Congress. In the short term, the effects of the mandatory cooperation of the private and public sectors of America can turn America into an unattainable power in the field of cyber defense and cyber attacks; Because the technical and technological ability of American companies in the field of cyber is more than any government, and what has caused such a comprehensive ability to not be provided to the government, is the commercial competition between these companies and prioritizing their economic profit. During his stay in the White House, not only has Trump not taken any action in this field, but he has also fired some positions and people who were working in this field. All this, along with his belief in the non-interference of Russia in the elections, has caused the Congress to change its position and take action. In 2018, Congress passed legislation to revive the Office of Cyber Diplomacy with defined functions and chaired by an ambassador-ranked individual, which requires Senate approval to take effect. Trump's and Congress's efforts in the field of cyber security will shape the future of cyber structures in the United States, which is under threat today more than ever before (20).

With the coming of Barack Obama, many plans and programs were proposed with regard to the evolution of cyber technology. He had several goals in mind to maintain America's cyber security and took more measures than George W. Bush. Examining his actions shows that he was very active in solving the cyber problems of this country and used all possible legal ways to develop policies related to this field. Despite this, America suffered bad security attacks during his presidency, such as the Russian cyber attack in the 2016 presidential election and several cases of organizational hacking. However, positive actions were also taken in the direction of change in this area and the domestic and international security environment. As the cyber space had become an important source of threat to the national security of America, the position of the national security strategy in the documents related to it also increased. One of the reasons why the Obama administration decided to update its strategy was that it did not consider what had been done so far to be enough. Therefore, there was a need for the Ministry of Internal Security and the National Security Council to organize not only for prevention, but also to prepare for a quick response to attacks to maintain national security. Therefore, it is more difficult to protect the citizens and the security of the country in the field of cyber because of its imperceptibility(21).

Table 2: Cyber processes and trends in American governments(20,21)

	President	Process
1	Bill Clinton	• Low dependence on cyber infrastructure •Economic opportunities of private companies • Most of the threats are severe and from government officials
2	Bush	•Increasing dependence on cyber infrastructure The emergence of terrorist groups as enemies The possibility of using computer programs as weapons
3	Obama	• Serious cyber attacks on American cyber assets and American companies Wide use of cyberspace by terrorist groups • Extensive casualties of the classic war
4	Trump	• The story of Russia's meddling in the election with cyber

		attacks Removing the Office of Cyber Diplomacy and the White House Cyber Coordinator Congress's reaction to Trump's actions in cyberspace
5	Biden	• Development of achievements and actions in the field of multiple intelligences

7. CONCLUSION

As mentioned, with the rapid growth of technology in the field of cyber space and the expansion of this field in many different aspects of life, this issue has become a vital issue for the national security of countries. All countries are particularly sensitive to the issue of their national security and are seeking to update it due to the rapid development of technology. Cyber technology is one of the strangest scientific fields today, and with the growth of this technology, the issue of cyber security and its connection with the national security of countries is becoming more prominent, so that it has become one of the concerns of all countries and organizations. With the development of this technology, the need for cyber security will become more prominent for everyone. The threats and dangers of this technology go in line with its positive aspects, and therefore the need for planning and policy making is also necessary for it. The connection of this technology along with artificial intelligence has multiplied the risks of this technology and this issue highlights the security aspect of this technology. In this research, it was shown that in each term of the presidency of American presidents, based on domestic and international needs and conditions, certain measures and policies were adopted and the strategies of each term were formulated based on it. During the presidency of George Bush, cyber defense and security of the country were considered. During the presidency of Barack Obama, the strengthening of cyber power and cooperation in all sectors and international cooperation was given special attention. The administration of Donald Trump also emphasized the fight and an aggressive approach to cyber security threats. The role of America's competitors as threats to the country's national security and cyber security is considered one of the important issues in these strategies. China, Russia, Iran and North Korea are specifically mentioned in some of these documents, and various cyber threats are They attributed and dealt with these countries through military and judicial means. Therefore, it is clear that with high-speed innovations in cyber space, the range of cyber threats will expand and cyber wars will become one of the most important aspects of combined wars. What is important for America and other countries is that it was a leader in the cyberspace and related technologies, and it is necessary to update it. Just as America has its own strategy for each organization and ministry, and each president specifies several strategies, other cyber powers are also moving in this direction. Finding weak points and security gaps, recognizing emerging threats and new governmental and non-governmental actors are among the dimensions that form part of the concern of the United States and other countries in the cyber future.

REFERENCES

[1] Ghasemi, Rooh A... and others (2016). Prioritizing the applications of Internet of Things technology in Iran's healthcare sector: a stimulus for sustainable development, Information Technology Management Journal, No. 1, 155-176

[2] Qureshi, Seyyed Ali, Shabro, Maryam (2013). An introduction to the application of Internet of Things technology in the smart network of the country's electricity industry, 29th International Electricity Conference, Tehran, Iran

[3] Valvi, Mohammadreza. Mohadi Sefat, Mohammad Reza and Bagheri Iman. (2016). Providing a strategic model for the migration of defense organizations to the cloud computing environment. Military Management Quarterly, 17th year, No. 1. pp. 106-130

[4] Halili Khodadad. Kazemi, Seyyed Mohsen and Dehghani, Mehdi. (2014). Examining security requirements and mechanisms in command and control systems based on cloud computing (CBC4I). The 9th National Conference of Command and Control of Iran. kharazmi University.

[5] Advisory Group on Public Diplomacy for the Arab and Muslim World. (2003). “Changing Minds, Winning Peace”, U.S. Dept. of State, Washington D.C. Available at: http://www.state.gov/documents/organization/24882.pdf, (Accessed at 1 October 2013).

[6] Barston, Ronald Peter, (2006), Modern Diplomacy, Cambridge: Pearson Education.

[7] Biener, Hansjoerg, (2003), “The Arrival of Radio Farda: International Broadcasting to Iran at a Crossroads”, Rubin Center Research in International Affairs, Available at: http://www.rubincenter.org/2003/03/biener-2003-03-02/, (Accessed at 2 March 2013).

[8] Bruce, Gregory, (2011), “American Public Diplomacy: Enduring Characteristics, Elusive Transformation”, The Hague Journal of Diplomacy, Vol.6, No.2.

[9] Clinton, Hillary, (2014), Hard Choices, Simon & Schuster Publication, London.

[10] Fialho, Lívia Pontes & Matthew Wallin, (2013), “Reaching for an Audience: U.S. Public Diplomacy towards Iran”, The American Security Project (ASP), Available at: https://www.americansecurityproject.org/ASP%20Reports/Ref%200131%20-%20US%20Public%20Diplomacy%20Towards%20Iran.pdf, (Accessed at 1 August 2013).

[11] Hanson, Fergus, (2012), “Revolution @State: The Spread of Ediplomacy”. Lowy Institute for International Policy, Available at: http://www.brookings. edu/~/ media/ research/files/reports/ 2012/3/ediplomacy%20hanson/03_ediplomacy_ hanson, (Accessed at 2 March, 2012).

[12] Jiang, Xiaoying, (2013), “U.S. Internet Diplomacy on China”, Master Thesis in China and International Relations, Aalborg University and University of International Relation, Available at: projekter. aau. dk/ projekter/ files/ 76941438 .

[13] U.S._Internet_Diplomacy_on_China_Xiaoying_Jiang

[14] Lydia, Gordon, (2009), “Regional Focus: Growing Internet usage in the Middle East and North Africa”, Available at: http://blog.euromonitor.com/2009/08/ regional-focus-growing-internet-usage-in-the-middle-east-and-north-africa.html, (Accessed at 4 August, 2009).

[15] Nweke, Eugene N, (2012), “Diplomacy in Era of Digital Governance: Theory and Impact”, Information and Knowledge Management, Vol. 2, No. 3.

[16] Congressional Budget Request”, Available at: https://www.bbg.gov/wp-content/uploads/2015/11/BBG-FY2015-PAR.pdf, (Accessed at 12 March, 2015).

[17] The Broadcasting Board of Governors, (2015), “Fiscal Year 2016 Congressional Budget Request”, Available at: https://www.bbg.gov/ wp-content/ uploads/ 2015/03/ FY2016 Budget_CBJ_Final_WebVersion.pdf, (Accessed at 8 March, 2015).

[18] The Broadcasting Board of Governors, (2016), “BBG Networks Provide Timely News of Iranian Nuclear Deal, Prisoner Swap”, Available at: nuclear-deal-prisoner-swap, (Accessed at January 21, 2016).

[19] Halili, Khodadad. Valvi, Mohammadreza. (2016). Big data technology, opportunities, challenges and strategies. The scientific research quarterly of interdisciplinary studies of strategic knowledge. The seventh year, number 28. pp: 7-28

[20] Majdi, Reza, (2023), Cyber Diplomacy towards Iran from 2006 to 2012, Publisher: Tehran City Publishing (affiliated to Tehran Municipality Cultural and Artistic Organization).

[21] Halili, Khodadad. Mazloum, Jalil and Hadian, Behrang. (2014). Investigating military applications of big data technology and its role in battlefield management. Quarterly Journal of Military Sciences and Techniques, Year 11, No. 33, pp. 47-62

[22] Halili, Khodadad. Sultanpour, Mohammad Reza and Mousavi, Fatemeh Sadat. (2014). The necessity of using big data technology in C4I systems and examining its challenges. The 9th National Conference of Command and Control of Iran. kharazmi University

[23] Halili, Khodadad. Valvi, Mohammadreza and Mohdi Sefat, Mohammadreza. (2016). Modeling C4I processes by physical-cyber-social systems (CPSS). The 10th National Command and Control Conference of Iran. Khatam La Anbia University (pbuh)