The Role of Artificial Intelligence as a Deterrent between the Iranian and Israeli Governments

Author's Details:

(1)Ehsan Afrashi; Master candidate of International Relations, Islamic Azad University, Bonab Branch , Bonab ,Iran **(2)Hamid Sarmadi ,** PhD in Political Science, Lecturer of Islamic Azad University, Islamic Azad University, Bonab Branch , Bonab , Iran.. (Corresponding Author). **(3)Javid karimi:** M.A of International Relations, Islamic Azad University, Islamic Azad University, Bonab Branch , Bonab , Iran.

Abstract

The main purpose of this study is to investigate the role of artificial intelligence as a deterrent power between the governments of Iran and Israel. Over the past few decades, the rise of the Islamic Republic in West Asia has changed the balance of power in the region. The Zionists have approached and introduced Iran as their main enemy. Meanwhile, the numerous attacks of the Zionist regime against the Iranian centers in Syria, mainly due to reasons such as the weak military position of the government of Bashar al-Assad and the limited military presence of Iran in Syria, have remained unanswered, which has caused the Zionist regime officials to continue these attacks. Follow with less concern and gradually expand attacks from Syria to Iraq, and even over the past few months, have prioritized cyber-attacks against the Islamic Republic of Iran. In this descriptive and analytical study, we seek to answer the question of what role artificial intelligence will play in the hands of the governments of Iran and Israel as a deterrent power. The cyber strategy of the Islamic Republic of Iran emphasizes the power of cyber-attack, which is influenced by the fact that Iran's cyber-attack power is at a very good level, but unfortunately Iran has invested limitedly in the field of cyber defense, which results in high cyber pollution and cybercrime. Cyber and, finally, successful cyber-attacks by other countries on Iran's vital facilities. In this regard, it is suggested that while continuing the cyber strategy of strengthening offensive power, increasing the strength of cyber defense should also be a priority.

Keyword: *Artificial Intelligence, Inhibitory Power; Israel, Iran*

1- Introduction and problem statement:

Artificial intelligence is one of the new achievements of human beings that can lead to a revolution in all aspects of human social and personal life. "Today, governments and private companies in specialized fields are trying to acquire the knowledge of artificial intelligence by using artificial intelligence in leadership. In the future, it will be the master of the world." This is an undeniable fact, and therefore there is intense competition among the great powers for progress in this field. Artificial intelligence has been used in various fields such as health, transportation, agriculture, databases, and defense and military. Utilizing the knowledge of artificial intelligence, like any new human experience, has been associated with a mixture of success and failure and positive and negative consequences, which has affected its development process (Mafi, 2006, 11)

Artificial intelligence, in short, leads to the production of machines that are capable of learning, understanding complex situations, thinking, reasoning, and providing answers and acquiring knowledge without the need for human help and intervention. Obviously, countries with such machines and systems can shift the balance of power in the international system to their advantage and form new alliances to intimidate enemies. Over the past few decades, the rise of the Islamic Republic in West Asia has changed the balance of power in the region, under the influence of which countries in the region have approached the Zionist regime to balance the threat and have identified Iran as their main enemy. The Zionist regime and the Islamic Republic of Iran have increased dramatically and unprecedentedly, so that the two sides seem to be practically in an escalating chain of crisis and war, which in the past few months, the Zionist regime has repeatedly stated the positions of Iran and its allies. It has targeted airstrikes in Syria and even in Iraq, played a role in the martyrdom of the commander of the Quds Force, and based on the available evidence, has repeatedly carried out cyber-attacks on Iranian infrastructure and facilities, such as the Natanz nuclear site and many others. Most importantly, contrary to the past practice and the doctrine of ambiguity of leadership that has prevailed in the Zionist regime for more than seventy years, the leaders of this country, especially Netanyahu, have confirmed their role in the

above actions in various ways. Other reasons for the Iran-Israel cyber war are low cost, secrecy and the weakness of international law in the field of cyber war. In addition to the above, Zionist officials are well aware that the Islamic Republic of Iran in the field of cyber warfare has put more of its power and capacity on cyber aggression and no other defense, which is one of the most important weaknesses of Iran in cyber warfare. As a result of this weakness, Israeli officials have identified Iran's vital infrastructure as the best target for cyber-attacks. Also, the internal situation in Iran and the special situation in the West Asian region are other factors that increase tensions with the Islamic Republic of Iran, because in the analysis of Israeli officials, the above trends are changing to the detriment of the Islamic Republic. Under the influence of US economic sanctions, of course, the Corona crisis, unemployment and widespread inflation have reduced the unity of Iranians and prevented cyber-attacks against Iran from uniting the people and the government. In the regional arena, Israeli officials have also analyzed this. It has been ordered that the influence of the Islamic Republic of Iran in the public opinion of the region is reduced and under the influence of the crisis of the Arab revolutions, it is Iran that is recognized as the main threat instead of the Zionist regime, as some Arab states including Saudi Arabia and the United Arab Emirates have sought to expand the Arab-Hebrew alliance with the Islamic Republic of Iran. (Arian, 2005, 8)

2- Theoretical foundations

Artificial intelligence

Artificial Intelligence, sometimes called machine intelligence, refers to the intelligence shown by machines in various situations as opposed to natural intelligence in humans. In other words, artificial intelligence refers to systems that can have reactions similar to intelligent human behaviors, including understanding complex situations, simulating human thought processes and reasoning methods and successfully responding to them, learning, and the ability to acquire knowledge and reasoning to solve problems. Most of the writings and articles related to artificial intelligence have defined it as knowledge of recognition and design of intelligent agents.

Artificial intelligence should be considered the vast expanse of meeting many old and new knowledge, sciences, and technologies. Its roots and main ideas are to be found in philosophy, linguistics, mathematics, psychology, neuroscience, physiology, control theory, probability, and optimization, and it has many applications in computer science, engineering, biology and medicine, social sciences, and many other sciences. (Farrokhzad, 2004, 10)

3- History of artificial intelligence:

Artificial intelligence in medical science Today, due to the spread of knowledge and more complex decision-making process, the use of information systems, especially artificial intelligence systems in decision-making, has become more important. The spread of knowledge in the field of medicine and the complexity of decisions related to diagnosis and treatment - in other words, human life - has attracted the attention of experts to the use of decision support systems in medical affairs. For this reason, the use of different types of intelligent systems in medicine is increasing, so that today the impact of various types of intelligent systems in medicine has been studied.

Artificial intelligence was introduced by philosophers and mathematicians such as George Bull, who proposed the laws and theories of logic. With the invention of computers in 1943, artificial intelligence challenged the scientists of the time. Under these circumstances, it seemed that this technology would be able to simulate intelligent behaviors.

Despite the opposition of a group of thinkers to artificial intelligence, who doubted its effectiveness, only four decades later did we see the birth of open chess machines and other intelligent systems in various industries. (Karshenas, 2006, 9)

The name artificial intelligence was coined in 1965 as a new science. Of course, activity in this field began in 1960. Most of the early research work in artificial intelligence focused on playing machine games as well as proving mathematical theorems with the help of computers. At first it seemed that computers would be able to

perform such activities only by using a large number of discoveries and searching for ways to solve the problem and then choosing the best way to solve them. (Nahazi, 1996, 199- 200)

The term artificial intelligence was first coined by John McCarthy (known as the father of intelligent machine manufacturing science). He is the inventor of one of the artificial intelligence programming languages called lisp. With this title, we can understand the identity of the intelligent behaviors of an artificial tool. (Man-made, unnatural, artificial) While artificial intelligence is accepted as a general term that includes intelligent and hybrid computations (composed of artificial materials). (Amini, 2005, 11)

4- Definition and nature of artificial intelligence:

To date, there is no precise definition of artificial intelligence agreed upon by scientists in this science, and this is not at all surprising. Because the category of mother and more fundamentally, intelligence itself, has not yet been defined comprehensively. In fact, we can find generations of scientists who have spent their entire lives studying and trying to find an answer to the major question: What is intelligence?

But most of the definitions offered in this context are based on one of the following four beliefs:

Systems that think logically

Systems that work logically

Systems that think like humans

Systems that act like humans

Artificial intelligence can perhaps be described as: "Artificial intelligence is the study of how computers can be forced to do things that humans are currently doing correctly or better" (Amini, 2004, 11)

A new and exciting endeavor to enable computers to think. Machines with real thought and sense of discernment (Hagland-1985)

A specialized field that seeks to explain and simulate intelligent behavior through computer processes. (Schalkov-1990)

The study of computations that enable machines to understand, reason, and act. (Winston - 1992)

The Ability to Achieve Human Performance in All Cognitive Cases by Computer (Alan Turing - 1950)

Artificial intelligence is the science and engineering of building intelligent machines, especially smart computer programs. Artificial intelligence is related to the same task of using computers to understand how human intelligence works, but it does not have to limit itself to methods that are biological. (John McCarthy - 1980)

5- Application of artificial intelligence:

Artificial intelligence has a variety of uses. Some of the most important applications of artificial intelligence include use in self-propelled vehicles (such as drones and self-driving cars), medical diagnostics, creating artwork, proving math theorems, brainstorming, image and sound identification, energy storage, web browsing, contracting, and Judicial rulings are foreseen. (Indic, 2003, 12)

6- History of artificial intelligence in the real world

Artificial intelligence has always been a topic of interest and engineers can use it as much as possible to improve their products and solutions. From the distant past you can find in various algorithms and technologies in this field. The military industry has always been a platform for the development of high-tech technologies. One of the first uses of artificial intelligence in the military industry was to use it to identify targets. The F14 models provided to the Iranian army in the years before the revolution have the ability to identify different targets, categorize them, and suggest them to the pilot. (Karami, 2015, 14)

In the military field, artificial intelligence has developed even more since then, and the issue of automatic weapons is one of the most controversial topics in all media today. Deadly weapons in which a robot is responsible for firing instead of a human. In other industries, due to the development of artificial intelligence, the use of this technology became popular. You may all remember that smile recognition technology was one of the most important things that was mentioned in camera and mobile ads for years. It was with the

development of the same technology that today we can apply various filters on our face on Instagram. You may be reading this article years ago, and the image filters we apply to our faces may seem as old-fashioned as smile detection technology. (Davis, 2002, 7)

7- Policymakers of the first generation of artificial intelligence

In the age we live in, we have seen for many reasons that artificial intelligence has grown by leaps and bounds. In fact, it is not all itself but other technologies that we can consider as the missing pieces of the all puzzle that have helped us make the most of all capacity. One of the things that has provided us with this capability is the development of mobile phones, as well as other sensors that continuously collect data from the environment and provide it to us for review. We have the opportunity to have very useful information about the behavior of individuals and citizens collected by smartphones. For example, the government today can easily measure the relationship between the effectiveness of public education (for example, the installation of billboards on a route of urban highways) and energy consumption (the rate of change in gasoline consumption of people traveling on that route) and using artificial intelligence Predict the appropriate frequency for advertisements and suitable places (Nani, 1998, 121)

Another issue that has led to the growth of artificial intelligence, which has been unprecedented in the history of artificial intelligence, is the ability to store information collected in low-cost, high-performance databases. Today, large databases have made it possible for information extracted from sensors by sensors to be stored on the cloud to be freely available to individuals. (Mahmoud Soheli, 2000, 17)

This is an important issue that you should not forget as a policymaker. There is one important point when we say that in our time it is possible to use databases, or that sensors can monitor and record information in different ways, and that is what we are talking about as a possibility. In many cases, it is not a technical feasibility, but a managerial feasibility. In the public sphere, the issue of artificial intelligence, although with a delay compared to the private sector, has been seriously considered. In fact, today we are at a point in the history of artificial intelligence that artificial intelligence as a tool is entering the administrative and political organizations and institutions. In the coming weeks, we will talk more about the public spheres in which artificial intelligence technologies have evolved, but as a case in point, check out the interesting example below (Roshandel, 1998, 110).

8- Inhibitory power of artificial intelligence:

How governments use artificial intelligence will have important implications for the field of international relations, and if a government has unusual power in this area, it can achieve such power that it threatens the very existence of other countries; For example, we can use the use of artificial intelligence to design and manufacture self-propelled weapons without the need to direct and control soldiers and the armed forces. Such weapons, which with their high intelligence automatically pursue the target until its final destruction, will be uncontrollable using traditional and conventional methods, and therefore the countries that benefit from them will change the balance of power at the global level. (Lochery, 2005, 54)

It is conceivable that some neighboring countries, which have had unresolved territorial disputes for decades, could use this new technology to gain an advantage over each other and destroy rival military might. Under these circumstances, if there is no law that obliges countries to refer to the arbitration and mediation of competent human beings to determine the final task regarding the performance and policy of various artificial intelligence tools, the continuity of human life is endangered; Because artificial weapons based on artificial intelligence will not be stopped until the pre-determined target is destroyed, the outcome of planning a military battle in such a way can be very dangerous. (Vest, 2002, 2)

Even if one country in the world leaves the determination of its military battle strategy entirely to artificial intelligence systems, one cannot expect other countries to leave the decision to humans; Because the processing power of the human brain is very limited compared to artificial intelligence machines, and this will lead to the

definitive military defeat of that country; As a result, the dominance of this mindset leads to unlimited competition for the deadly weapons of artificial intelligence in the world, which will result in nothing but the death and annihilation of humanity. In this situation, the category of ethics becomes a luxury commodity that no country will care about except in words. (Khatibzadeh, 2002, 407- 420)

Another concern is that artificial intelligence-based military systems, as well as world military decision-making systems based on the use of artificial intelligence weapons, will eventually rapidly marginalize existing approaches to the peaceful resolution of political and economic disputes. Today, some international institutions as well as global regimes, treaties are designed to help disarm, prevent the proliferation of weapons of mass destruction, international mediation, etc., which are in line with the technological conditions of the world in the twentieth century and keep pace with world scientific developments. Therefore, these mechanisms will practically lose their efficiency and effectiveness in the era of artificial intelligence, which has not been very significant before (Shah Karami, 2001, 13).

The advancement of AI weapons can also help destructive role-playing for non-state actors who, unlike governments, are not required to act transparently and responsibly on the world stage; For example, these actors, especially unidentified terrorist groups, can use smart drones and cheap cars to kill their opponents quickly and cheaply and unleash unbridled international unrest. Weapons based on artificial intelligence enable non-state actors to line up against the massive military equipment of the world's classic armies that are not yet equipped with this technology, and even to achieve achievements that were previously unimaginable for them. (Mekay, 2004, 2)

9- New wars with artificial intelligence

Battles based on the use of AI weapons will not be limited to the physical realm, but will also make cyber-conflict more difficult and deadly; For example, hostile non-state actors or actors will be able to design machines and tools that automatically infect critical infrastructure, control and command systems, etc., and automatically invent malware and viruses to propagate them to target centers. (Weston, 2002, 2)

The misuse of artificial intelligence will not be limited to the realm of hard power or cyberspace, and will extend to areas such as the media. Artificial intelligence systems can be used to wage psychological warfare, to design fake but effective news, to manipulate public opinion in the target countries, to produce fake news and information videos, and so on. Artificial intelligence makes it possible to design videos in which any speech can be attributed to any celebrity or politician, and it is possible to manipulate the facial expressions and voices of people to make the sentences attributed to them believable; For example, this technology can be used to produce a fake video in which the president of a country launches violent attacks against another country and comments with inappropriate literature against the officials of that country. Such actions could have irreparable consequences for international peace and security, and encourage senior officials to do things that are not in their national interest by arousing their emotions. (Ibid, 2)

We are witnessing the first manifestations of the abuse of artificial intelligence in the field of soft power and the media by publishing a lot of fake news, especially on social networks in the run-up to the presidential, parliamentary and other elections in different countries. The most controversial incident in the months leading up to the 2016 US presidential election took place, during which a lot of fake news aimed at destroying Hillary Clinton was published on social networks, and it was later claimed that a large part of this news and information was supported by users. The Russian government has published on the Internet. Events like this can disrupt the functioning of liberal-democratic systems and hold elections, and reduce people's trust in the political systems and their constituencies in different countries. (Asher, 2003, 3)

In such circumstances, it becomes necessary to review arms control strategies, non-proliferation and non-proliferation, media strategies, etc., and coordination and knowledge of the foreign policy of rival countries becomes more important; Because the slightest misunderstanding can lead to very destructive wars between neighbors as well as between governments and non-state actors. (Gold, 2007, 4)

At present, most governments and many politicians have little information about the new functions of technology, especially artificial intelligence and its impact on various aspects of human life, and even consider related issues unimportant, luxurious and fantasy. At the same time, governments that have begun to design AI initiatives and strategies pay little attention to the red line in this area and do not think about how to use AI technologies responsibly to comply with international law and peaceful coexistence of the nation-states together can be possible. (Baroud, 2008, 3)

The emergence of artificial intelligence, given these challenges, poses fundamental problems for the future of political systems, and especially for liberal-democratic systems and institutions, and even threatens equality and social order; because advanced AI-based control and monitoring systems can easily find and identify any person at any time and place, leaving no privacy for people. Under these circumstances, issues such as human rights and civil liberties are marginalized and living freely in human societies becomes a dream. Avoiding the deepening of some of these challenges it is the duty of diplomats to devise an acceptable mechanism for the use of artificial intelligence technology through international negotiations and the deepening of communication. (Kasraei, 2007, 14)

10. Artificial intelligence in politics

The application of artificial intelligence in political science is one of the issues that has been considered. According to researchers at the University of Massachusetts, one example of the use of artificial intelligence in politics is the production of a writer robot that can write plausible political speech. The group used Google n-gram technology to build artificial intelligence. 4,000 speeches delivered in the US Congress have been used to teach artificial intelligence. (Sabeti, 2007, 13)

According to the results of Dr. Mehdi Motaharnia, a university professor and political futurist, in the article "The Relationship between Artificial Intelligence and Politics", it can be said: "As politics is now affected by economy, culture, ecology and security issues, it must be said that artificial intelligence It will affect all of these areas, and by affecting all of these areas, it will change various aspects of our lives in social, ecological, economic, cultural, military, security, and even legal matters. "

Considering the wide and deep scope of the impact of the entry of artificial intelligence into the field of politics, the field of politics and its impact on artificial intelligence should be examined. (Hamid, 2006, 4)

11 - Application of artificial intelligence in foreign policy

As countries turn to artificial intelligence and algorithms to predict events, countries' foreign policies will change dramatically as countries interact with each other knowing that their every move may be predicted days, weeks or months in advance.

Such a transformation will transform the world of business and geopolitical relations.

(Reza Majidzadeh - Development Expert)

The world of politics is like a game of chess, based on evaluating scenarios and predicting the best reaction or the best move of the pieces; But the chess of the political world is more complex; As many actors with overt and covert preferences participate in that their declared and applied approaches are not necessarily the same; Internal changes in countries' policies, including shifting power and changing the structure of rent resources, affect the strategies, tactics, and behavior of actors, and ultimately, it is difficult to understand the distinction between signal (signaling a particular motivation or belief), information, and foreign policy analysis. The complexity increases when all of these points need to be considered in a future-oriented analysis in order to adopt an appropriate foreign policy. In futures research methods, simulation methods based on artificial

intelligence, game modeling and scenario writing are more capable in terms of presenting possible future images, prioritizing, determining drivers, explaining cause-and-effect relationships and the possibility of designing a foreign policy mechanism. Nowadays, computer software and artificial intelligence have increased the possibility of accurately using these analytical tools to design and advance foreign policy. (Chomsky, 2008, 10)

12- Artificial intelligence and foreign policy

At a time when foreign policy is moving toward algorithms that aim to analyze data, predict events, and consult with governments, artificial intelligence can be used in a variety of foreign policy areas. Managing public expectations in another country, making decisions based on scenarios and analyzing the signals received from speeches and positions of other countries' officials are among the most important applications of artificial intelligence in foreign policy. Of course, a correct understanding of the subject under analysis in foreign policy takes precedence over the choice of an applied model and the type of use of artificial intelligence tools. In the same vein, two years ago, China unveiled a new artificial intelligence system designed specifically for its foreign policy. The system, called the "Geopolitical Environment Prediction and Simulation Platform," offers foreign policy proposals to Chinese diplomats after analyzing large amounts of data. According to an informed source, China has already used a similar system to accurately evaluate all its foreign investment projects over the past few years. Another widely used international artificial intelligence system that has been used in Iran is the artificial intelligence approach based on simulation of games and strategic confrontations that uses various software such as GMCR and Bruno di Muskita integrated software. The GMCR software was first developed in the Canadian Ministry of Defense but is later used in civilian but conflict of interest contexts, and its current version, GMCR +, has civilian intellectual property. (OpallRome, 2001, 2)

Bruno Muskita, known in Iran for predicting the results of the 2009 presidential election, is a foreign policy adviser in the United States who has provided a combined model of Bayesian games for foreign policy analysis and prescribing. The purpose of this model is to predict the processes and outcomes that lead to negotiations or political situations that lead to conflict, war, agreement, or disintegration. This model is used for situations of threat and negotiation or the possibility of war in the international arena, domestic politics or even social and business relations. It is necessary to analyze the actors, their possible actions and current, short-term and long-term evaluations of the trends, tactics and beliefs of the game stakeholders. Of course, in addition to the basic grammar of game theory, some innovative and heuristic rules are also used for calculations. These innovative rules are combined with the principles of game theory to get a more realistic picture of the interaction situation. (Benozadok, 2002, 140-142)

Thus, in today's world, foreign policy will change dramatically as countries turn to artificial intelligence and algorithms to predict events. Because countries will interact with each other knowing that their every move may be predicted days, weeks or months in advance. Such a transformation will transform the world of business and geopolitical relations. In such circumstances, artificial intelligence helps to determine the assumptions based on the panel of experts from foreign policy experts (and other areas as needed, such as social psychology, political sociology). , Anthropology, etc.), identify the type of each actor and his different choices based on this type, and then artificial intelligence, calculate and prioritize different scenarios. For example, there are eight articles that have analyzed and predicted the Iran-US confrontation over Iran's nuclear program and its possible scenarios using this model. Although the results of the use of artificial intelligence do not mean their certainty, but by using artificial intelligence tools, the degree of uncertainty in the design and promotion of foreign policy can be reduced and the best strategies can be adopted (Website of the Strategic Council on Foreign Relations, 8th of July, 2020)

13-Artificial intelligence in Iran:

In today's world of globalization and its aftermath, the writings of thinkers such as Joseph Nye and Robert Cohen on new forms of power and new means of influence have become increasingly important. It should be noted that the Islamic Republic of Iran, due to its cultural power, historical richness and efficient human

resources, has a comparative advantage over many countries in the region in the use of soft power (knowledge, culture and ideology). Ancient history and long-standing and influential Iranian civilization in the region and the rich culture arising from it, has always been one of the significant and effective factors in Iran's presence in regional relations. To other countries, in practice, the Islamic Republic of Iran began to use soft power, but from the very beginning of the revolution, Iran faced many challenges such as war and sanctions, etc., which made the strengthening of hard power become the first priority of the statesmen, but with the reduction of these problems and all-round progress of the Islamic Republic of Iran, We are now witnessing that the strengthening and use of soft power, as a low-cost but effective power, has become an important principle in the view of Iranian politicians.(Rahmani, 2007, 11)

It is a powerful country that has more potential resources in soft power and the ability to use it properly. Considering that the Islamic Republic of Iran has a comparative advantage in knowledge, culture and ideology over the countries of the region, and politicians, according to the Vision 1404 document, are also aware of its importance and have benefited from it; therefore, the Islamic Republic of Iran has strengthened and promoted its regional position by using soft power. (Miley, Mohammad Reza and Matiei, Maryam, 11/25/2016)

14. Artificial intelligence in Israel:

The civilian and internal dimensions of the Zionist regime are unknown to many Iranians. Given the importance of the role of technology, the Zionist regime has pursued various policies to support technology. The Zionist regime has appointed two ministries of economy and science, technology and space to develop technology and inventions. The Ministry of Economy, which focuses on the development of economic growth in the Zionist regime, has specifically established the Office of Senior Scientists to implement policies and programs to support and encourage industry research and development. The agency implements various programs to encourage technology entrepreneurs and in order to increase the scientific resources of the Zionist regime based on industry and development, undertakes research and development cooperation at the national and international levels. The Ministry of Economy has also established an investment development center to develop local and foreign investment in the technology and inventions industry. The center encourages foreign investment in the Zionist regime and the development of cooperation with foreign companies. To achieve these goals, the center acts as an information and coordination center. The Ministry of Science, Technology and Space is also responsible for identifying and funding technological and scientific research, providing scholarships for graduate students, and encouraging scientific cooperation with other countries and international organizations. The Zionist regime has also provided local and foreign investment incentives for industrial projects with a variety of incentive offers through the Investment Promotion Act. As a result of government incentives, many international companies have joined the Zionist regime. For example, companies such as Microsoft, Cisco, Hilot Packard and Time Warner have established research and development centers in the Zionist regime.(Estimation Monthly, Nos. 66 and 67, September and October 2018; 43)

15- The role of artificial intelligence in Iran-Israel relations:

Over the past few decades, the rise of the Islamic Republic in West Asia has shifted the balance of power in the region which under the influence of that, the countries of the region have approached the Zionist regime to balance the threat and have introduced Iran as their main enemy. The next issue is the regime's strategy. Zionist turned against the Islamic Republic of Iran, the defenseless skies of Syria and Iraq and of course the support of world powers such as European countries and the United States with Zionist regime airstrikes on Iranian positions in Syria and Iraq and of course the lack of opposition to such attacks by Russia. Meanwhile, the numerous attacks of the Zionist regime against the Iranian centers in Syria, mainly due to reasons such as the weak military position of the government of Bashar al-Assad and the limited military presence of Iran in Syria have remained unanswered, which has caused the Zionist regime officials to continue these attacks. They should follow with less concern and gradually expand their attacks from Syria to Iraq, and even prioritize cyber-attacks against the Islamic Republic of Iran over the past few months. However, in the past few months, there

have been widespread cyber incidents in the country, based on available evidence, including unofficial reports published in the Zionist media, as well as remarks heard by Zionist officials; it has been given priority by this country against the Islamic Republic. In this regard, we can refer to a report published in a Zionist regime media. "In the last three weeks, Iran has witnessed mysterious explosions in wide ranges, sparks of light and intense tongues of fire and smoke clouds that stretch far and wide," Zionist Channel 13 TV reported in a report on July 20. Iran's nuclear sites, military bases, military-industrial plants, oil pipelines, power plants and other places have been repeatedly set on fire and exploded. According to this report, the tension behind the curtain has been at a higher level in recent days after a long period and years after the stochastic virus and the assassination of Iranian scientists; these events may not have been accidental, and a very obvious and difficult war has unfolded. The report says that the Iranian people are facing a new war, in addition to the economic collapse, inflation, rising unemployment and the outbreak of the Corona virus which has targeted them brutally. According to the network's reporter, however Iranians are still unaware of exactly what is going on in their country, and the explosions have taken them by surprise in an unprecedented way. According to this report, Tehran is becoming like Damascus. Iranians, who did not know such a fact before, are waiting for the sparks of the explosion every night with a mobile phone camera on and looking at the sky to record it. According to Zoe Yakhzaql, the report's author, the blasts could be a series of random events, but perhaps someone has declared war on Iran, and someone in the Middle East is using the principle of "trampling on the weak."

This network lists 14 explosions in 21 days on the map of Iran and in the order in which they occurred as follows:

June 26: Explosion in Parchin near a site suspected of conducting a nuclear test; Explosion in Khojir forest;

June 26: Fire in Shiraz power plant;

July 1: Explosion at Sina Athar Clinic in Tehran;

July 3: A major explosion at the Natanz nuclear site in Isfahan damages Iran's uranium enrichment process;

The evening of July 3: Another fire in Shiraz;

July 5: Explosion and fire at Madhaj Zargan power plant on the outskirts of Ahvaz;

July 5: Explosion, fire and chlorine leak in Karun Mahshahr Petrochemical Complex;

July 5: Suspicious incident in Tondgouyan Petrochemical Complex;

July 8: Explosion in a factory in the south of Tehran;

July 10: An explosion in western Tehran that resulted in power outages in two neighborhoods, including the city of Quds;

July 13: Fire in Tondgouyan Petrochemical Complex;

July 14: A fire leads to an explosion in a gas condensate factory in Kavian town in Fariman Khorasan;

July 16: Massive fire in Bushehr launch factory;

July 20: Power plant explosion in Isfahan province. Another evidence of rising tensions between the Zionist regime and Iran is a set of military-intelligence developments that show an unprecedented increase in the readiness of the Zionist army to confront the Islamic Republic of Iran. In this regard, we can mention the formation of a new drone unit and the third ring in the Zionist regime. In late June, the Israeli army launched its new drone unit within the framework of the secret operations unit of the army 9900 unit. Unit 9900 is responsible for collecting geographic visual data under the Zionist Army Intelligence Department. According to Israeli intelligence officials, in addition to strengthening electronic warfare capabilities, the new drone unit will be set up with the aim of gathering security and military information more accurately and quickly to provide the information needed by soldiers on the battlefield and will "double" the unit's capabilities.

The commander of the unit said that the forces of the army's ground and armored units can guarantee their superior capability during operations and on the fronts through fast and updated information of the UAV unit in any climatic conditions. The formation of a new drone unit in the service of the 9900 Secret Unit is part of the implementation of a plan called "Tanufa" or "Momentum" that Avio Kukhawi, the chief of staff of the Zionist regime, last year to strengthen the destructive power and strike against the army of the regime with cross-border threats and threats from Iran. At the same time, Zionist officials announced that a new body in the Zionist regime's army, which was to be set up under the name of Strategic Administration and Iran to confront the

Islamic Republic of Iran had removed the name of Iran and chosen the title of "Strategic and Third Circle". "Third Circle" refers to cross-border threats mainly from Iran in the region and beyond to the Zionist regime, as well as similar threats from other countries. Despite the removal of Iran's name from this part of the army, the Zionist regime's media have reported that the process of selecting officers for this institution is still ongoing. (Buchanan, 2006, 3)

The Israeli Ministry of Defense announced in a statement in July 1999 that it had successfully launched the OFAC 16 reconnaissance satellite in cooperation with the Israeli aerospace industry. The statement did not provide details about the OFAC-16 mission, but Israeli radio said that OFAC-16 was in orbit to monitor Iran's nuclear activities. The satellite was launched with a Zionist rocket made by the Zionist regime and was successfully placed in the space provided. The Ministry of Defense of the Zionist regime called the launch of this satellite another extraordinary achievement and said that the superiority of technology and intelligence capabilities is vital for the security of the Zionist regime. "We continue to strengthen and maintain the capabilities of the Zionist regime on all fronts and in all places," the statement said. Shalom Sudari, the head of the Zionist Aerospace Industries Space Program, said: "The Zionist satellite network allows us to observe all the countries of the Middle East and beyond." The Israeli Ministry of Defense described the OFAC 16 as an electro-optical reconnaissance satellite with advanced capabilities and said that the first images would be received in about a week. The last satellite of this type, called OFAC 11, was launched in September 2016. It should be noted that the launch of the OFAC 16 satellite coincided with an explosion at Iran's advanced centrifuge assembly center at the Natanz nuclear facility, in which the possibility of Israeli involvement was raised, but not confirmed. However, the launch of the OFAC 16 satellite with the aim of monitoring Iran's military and nuclear activities, along with the explosion at the Natanz nuclear site, are other signs of the escalating cycle of crisis between the Zionist regime and Iran and increasing the likelihood of military conflict (Lali, 2008, 15).

16-Cyber-attacks against the Islamic Republic of Iran

As it has been said, in 2020, the Zionist regime officials for various reasons have expanded cyber-attacks and sabotage against the Islamic Republic of Iran, and Iran has responded to them; In a way, it seems that the trend of cyber-attacks and sabotage of the two sides against each other is so increasing that it may eventually and perhaps unintentionally lead to a wider cyber and even military war. In any case, for Iran and the Zionist regime, the red lines of each other are not very clear, and at any moment it is possible for one of the parties to cross the other red lines and the existing crisis inadvertently enters into a full-scale war; For example, a cyber-attack or sabotage on the Natanz site or a cyber-attack on the Zionist regime's water and sewage system may have been an attempt to estimate the other side's tolerance and red line. Based on this, what is clear is that the process of increasing tensions between the Zionist regime and Iran is increasing rapidly. Under the influence of these circumstances, the question arises as to why cyber warfare has been widely and of course unusually prioritized by the Zionist regime at this time and for what purposes. (Rose, 2008, 3)

As mentioned earlier, the prioritization of cyber warfare against the Islamic Republic of Iran has far-reaching implications, ranging from the revelation of Iran's nuclear program to Arab developments, particularly in Syria and Iraq, but what has resulted in a few months. In the past, tensions and cyber warfare have become unusual phenomena, one being the internal situation of the Zionist regime and the other worrying about the possible outcome of the new US administration negotiating with Iran. (Ritter, 2006, 4)

In this regard, it should be noted that the internal situation of the Zionist regime has always played an important role in the policies of this country towards the Islamic Republic of Iran. Zionist officials consider Biden's victory and possible return to Borjam to mean the normalization of the situation in the Islamic Republic of Iran and the country's escape from the internal and regional crisis. Under the influence of these circumstances, it

seems that the priority of a large-scale cyber war against the Islamic Republic of Iran is to strike at its nuclear program, at a time when Iran is facing internal and regional problems, and according to Zionist regime officials, the situation it has a weakness. (Logon, 2006, 11)

Another analysis in this regard was that the Zionist regime officials sought to increase the tension with the Islamic Republic of Iran in order to force it to respond before the US elections, which resulted in a limited or extended conflict with the US. Zionist officials have prioritized a strategy of escalating tensions against the Islamic Republic to increase the likelihood of the country clashing with the United States. Meanwhile, the arms embargo against the Islamic Republic of Iran has recently ended and the United States and the Zionist regime have not been able to bring together powerful countries, including members of the Security Council, to extend arms embargoes against Iran, and have acted unilaterally in this regard. In such a context, increasing tensions and limited conflict could strengthen that diplomacy and bring powerful states closer to the United States. (Kelman, 2007, 29- 40)

At the same time, the escalation of tensions with Iran, which is followed by cyber-attacks and sabotage, could provoke a reaction from the Islamic Republic and reduce cooperation with the Atomic Energy Agency, which in turn will increase tensions between Iran and the United States. This is the path. Of course, there are other reasons for prioritizing cyber warfare against the Islamic Republic of Iran in the current context. As mentioned, efficiency, concealment of the attacker, weakness of international law and weakness in the cyber defense of the Islamic Republic of Iran are among the reasons for this. (Abunimah, 2007, 2)

The first point is that cyber warfare does almost what military warfare does at a lower cost. The experience of cyber warfare over the past few years shows that leading cyber governments can use widespread malware to wreak havoc on their target or targets. Therefore, the first point is the destructive power and efficiency of cyber warfare. The second point is that unlike a military attack, in a cyber-attack the attacker can hide and not pay much for it. In addition, in the field of international law, the law governing cyber warfare is not very advanced, and countries such as the Zionist regime are taking full advantage of this legal vacuum. Finally, the cyber strategy of the Islamic Republic of Iran emphasizes the power of cyber-attack, which is due to the fact that Iran's cyber-attack power is at a very good level, but unfortunately Iran has made limited investment in cyber defense, which results in high pollution. And cybercrime, cyber sabotage and, finally, successful cyber-attacks by other countries on Iran's vital facilities. In this regard, it is suggested that while continuing the cyber strategy of strengthening offensive power, increasing the strength of cyber defense should also be a priority. (Sadeghizadeh, 2007, 51-53)

17- Analysis of Western experts on the increase of tension and bilateral cyber-attacks

The analysis of the Zionist regime's experts on the reasons for the increase in tension and cyber-attacks with the Islamic Republic of Iran has a wide range. As an example of a different analysis, we can refer to an article about the Zionist regime's attack on the port of Shahid Rajaee, which was published by the New York Times. The authors of this report believe that the cyber-attack of the Zionist regime on Shahid Rajaei port, which is one of the most important international transit corridors in the world, which alone accounts for more than 55% of exports and imports and 70% of transit of the country's ports (Sadeghizadeh, 2007, 8)

It is designed to deter the new cyber-attacks of the Islamic Republic of Iran. In fact, the key point of the above article is to emphasize that the Zionist regime does not seek to increase cyber tensions with the Islamic Republic of Iran. Accordingly, the authors of the article, in conversations with Israeli intelligence agents, have concluded that the most important goal of the Israeli cyber-attack on the port of Shahid Rajaei is to prevent Iran from further cyber-attacks. To prove this, intelligence officials have provided several clues.

1. First, the Zionist regime's counter-cyber-attack was carried out immediately and with the least amount of time to make it clear that the Zionist regime has the necessary plan and power to harm Iran.

2. Secondly, the attack took place in a place that is important for the Islamic Republic of Iran and is one of the main bottlenecks in Iran's foreign trade to clarify the serious determination of the Zionist regime. The third point is that the cyber-attack was on a very limited level and was designed in such a way that there were no casualties to reveal that the only purpose is to threaten and detain Iran. It should be noted that the cyber-attack delayed the transfer of ships to Shahid Rajaei port for only a few days, but did not cause serious damage. The next point is that the Zionist regime officials, contrary to the previous procedure, admitted in various ways that they had carried out a cyber-attack. (Washington Monthly, No. 91, October 2020; 72) The Washington Post also claimed that this attack was in response to a cyber-operation by Iran In April, it was called the "Rural Water Facility of Israel" (Islamic Republic News Agency website; May 19, 2020). However, the authors of the article believe that the Islamic Revolutionary Guard Corps will continue its cyber-attacks; because the IRGC officials know how vital the infrastructure is, especially the issue of water, for the Zionist regime. For this reason, the Chief of General Staff of the Israeli Army, Aviokhawi, has emphasized that all available tools and all innovative methods will be used to confront Iran. Among other things, he believes that the Zionist regime has an intelligence and military superiority over Iran and will be successful in any war. The key point of the article, which is somewhat lost in the text, is that the Zionist regime, despite its military, intelligence and cyber superiority over Iran, is vulnerable to cyber-attacks in the field of critical infrastructure, including water. In other words, despite its strategic superiority in the field of cyber, the Zionist regime is one of the most vulnerable countries in the world in the field of cyber threats due to its geographical conditions and high sensitivity to costs and damages (Aoun, 2006, 3).

3. The recent cyber-attacks targeted the citizens in a new trend which was unusual in the dispute between the two sides. This can be dangerous for people on both sides; For example, the lack of access to safe water for the citizens of the Zionist regime or the sabotage of Iran's exports and imports can disrupt the import of food or health items that are essential for the Iranian people.

4- Cyber-attacks on important centers are considered for both sides of the red line, which can have unexpected results and actually lead to escalation of tension and war; There is also a serious miscalculation in the field of cyber warfare.

5. The Zionist regime is a global power and Iran is a growing power in the field of cyber.

6. The above attacks showed weakness in the field of cyber defense and cyber deterrence. (Montazeri, 2007, 10)

Conclusion:

Cyber warfare is becoming the most effective tool in the hands of countries that intend to cause serious harm to their enemy due to its many positive features such as high efficiency and low cost. In this regard, the Zionist regime officials, under the influence of Iran's internal trends, special conditions in the region and concerns about returning to the United States, consider cyber warfare against the Islamic Republic of Iran as the most effective tool to achieve its goals, including damaging the republic's nuclear program. Islamic Iran has been evaluated. In this regard, in the past few months, the Zionist regime has increased military attacks on Iranian forces and regional allies of the Islamic Republic in West Asia, and with numerous cyber-attacks has tried to delay Iran's nuclear program and increase the level of crisis. In such a situation, what is important for the Islamic Republic of Iran is to try to increase solidarity in different parts of the system and to create solidarity between the people and the people with the government and to avoid increasing tensions. Of course, the key point is to return to the UN Security Council and the US agreement with Iran in the future, the outcome of which could have far-reaching implications for the state of extended sanctions and the strategy of comprehensive pressure. Finally, what can be deduced from recent events is the widespread importance of discussing cyber defense alongside cyber-attack power.

References:

A. Persian references:

- Arian, Reza (3/30/2005), "Reforms in the Middle East; Inevitable", Democracy.

- Amini, Hassan (25/8/2004), "Virtual Democracy, Real Dominance; Analysis of America's New Plan for the Middle East", Jam Jam.

- Indic, Martin (March 31, 2003), "Four Axis in American Middle East Politics", translated by Hassan Hashemian, Iran.

- Sabeti, Vahid (7/5/2007), "Israel; lost in the sixth war", Nowruz.

- Chomsky, Noam (29/4/2008), "Israeli urban planning programs; failed states", translated by Yaqub Nemati and Rojni, Jam Jam.

- Hosseini, Emad (11/13/2007), "Israel did not win the war; Vinograd reports about the war", brokers.

- Khedrlou, Mohammad Reza (6/1/2005), "Free Trade of the Arab League", World Economy.

- Khatibzadeh, Saeed (Summer 2002), "Turkey and Israel; Efforts to Find a New Security-Political Framework", Foreign Policy Quarterly, No. 20, 16th Year.

- Roshandel, Jalil (Summer and Autumn 1998), "Turkish-Israeli Security-Military Pact", Middle East Studies Quarterly, Nos. 2 and 3, 5th Year.

- Rahmanian, Maryam (2/5/2005), "Erdogan's visit to Israel and Palestine", East.

- Rahmani, Mohsen (16/8/2007), "Looking back at the 33-day war", Mardomsalari.

- Shahkarami, Maryam (11/8/2001), "Military-Security Cooperation between Turkey and Israel", Aftab Yazd.

- Sadeghi, Ahmad (November 2005), "Knowledge of Islamism", Monthly of the Office of Political and International Studies (Views and Analysis), No. 191.

- Sadeghizadeh, Kasra (8/5/2007), "Israel after Vinograd", Resalat.

- Alikhani, Saeed (6/11/2007), "Olmert Iron Shield Plan; the Second Strategic Mistake after the 33-Day War", Iran.

- Fath Ali, Hassan (3/1/2008), "Arab gathering to resolve the Lebanese crisis", Jahan Sanat.

- Farrokhzad, Farshad (21/9/2004), "American Democracy; Foreign to the Region", Jam Jam.

- Kasirov, Dmitry (10/4/2008), "Arab Union Suspended between Disintegration and Cohesion", translated by Mohammad Ali Firoozabadi, Kargozaran.

- Karshenas, Massoud (4/17/2006), "Economic Reforms in the Middle East", Kargozaran.

- Kasraei, Shaker (28/5/2007), "33-day war and the great crisis of the Zionist regime", Islamic Republic.

- Krobungard, Anthony (December 2000), "Commodity water of feathers in the Middle East", translated by A. Hedayati, Economic Translator, Nos. 9 and 10.

- Karami, Ali (11/10/2005), "America's Challenges in the Reform Process in the Middle East", People's Way Magazine.

- Lugon, Jean François (22/7/2006), "Israel's real goals; beyond Gaza and Beirut", East.

- Lali, Alireza (April 2008), "International, regional and domestic consequences of the 33-day war", Khorasan.

- Mahmoud Sohli, Nabil (23/3/2000), "Increasing US aid to Israel", translated by Ismail Iqbal, Lebanese daily Al-Mustaqbal.

Maleki, Mohammad Reza (Winter 1998), "Turkey-Israel Relations and Its Effects in Central Asia and the Caucasus", Quarterly Journal of Central Asia and Caucasus Studies, No. 24, Volume 3, 7th Year.

- Mohtasham, Mohieddin (13/6/2007), "Comparative comparison of the 6-day Arab war and the 33-day war of the parties ..." the party....

- Montazeri, Ali (7/8/2007), "From the 33-day war to the 33-day conference (Kouchner plan)", selection.

- Mafi, Katayoun (14/8/2006), "The Rise of the New Middle East without American Planning", Jam Jam.

- Nahazi, Gholam Hossein (1996), "Water Crisis in the Middle East", Quarterly Journal of Middle East Studies, No. 1, second year.

- Nani, Julia (Spring 1998), "US Security Perspectives and the Transfer of Energy from the Caspian Basin", translated by Vajihe Sadeghian, Quarterly Journal of Central Asia and Caucasus Studies, No. 21, 6th Year.

- Hedayati, Bahman (6/8/2008), "Victory without martyrdom operations", party....

B. Non Persian references:

- Asher, Arian (October 2003), "Israeli Public Opinion on National Security 2003", *Jaffa Center for Strategic Studies Memorandum*, No.67, available at: www.tar.ac.il.

- Abunimah, Ali (3 February 2007), "The American Proxy war in Gaza", available at: *www.ifamericansknew.org/cursit/proxywar.html*.

- Aoun, Elias (17 July 2006), "Israel's Real war objectives", available at: *www.alhewar.org*.
- Benozadok, Efraim (winter 2002), "State- Religion Relations in Israel the Subtle Issue

Underlying the Rabin Assassination", *Israeli Affairs*, Vol.8, No.182.
- Buchanan, J. Patrick (August 15, 2006), "Olmert's War and the Next One", available at: *www.antiwar.com*.

- Baroud, Ramzy (4 June 2008), "Life after Bush: Forecasting Peace in Palestine", available at: *www.counter Currents.org/palestines.htm*.

- Chomsky, Noam (March, 2005), "Promoting Democracy in the Middle East", available at: *www.countercurrents.org/iraq-chomsky 060305.html.*

- Davis Hanson, Victor (October 2002), "Democracy in the Middle East", Vol.8, available at: *www.weekly standard.com*.

- Gold, Dore (23 November 2007), "Towards Annapolis: Is U.S. Policy Changing on Israel's Rights in a peace settlement?" Vol.17, No.22, available at: *www. jcpa.org*.

- Golan, Galia(2008), "1948: Sixty Years After", The Evolution of Israeli Policy on the Israeli- Palestinian Confilict, Vol.15, No. 1&2, available at: *www.pij.org*

- Hamid, Shadi(3 August 2006), "The Sixth war: 1948, 1956, 1967, 1973, 1982, and, apparently, available at: *www.democracyarsenal.org*

- Kelman, C. Herbert (Fall 2007), "Israeli- Palestinian Peace: Inching Toward Looking Beyond Negotiations", *Middle East Policy*, Vol.14, Issue 3.

- Kelly, Lorelei (3 August 2006), "Hezbollah, Israel and Responsibility to protect", available at*: www.democracyarsenal.org*

- Lieven, Anatol (Spring 2007), "Iraq, Iran, Israel and Eclipse of U.S. Influence: what Role for U.S. Now?" *Middle East*, Vol. 14, Issue 1.

- Lochery, Neill, "Israel and Turkey", Depending ties and Strategic, Implications", *Israel Affairs*, 2005.

- Mekay, Emad, "Iraq war launched to Protect Israel- Bush Adviser, *Inter press service*, March 29, 2004, at: www.ifamericansknew.org

- Opall Rome, Barbara (15 November 2001), "U.S. Israel plan closer political- Military ties", *Defense news*.

- Rose, David (April 2008), "The Gaza Bombshells", *Vanity Fair*, available at: www.ifamericansknew.org

- Ritter, Scott (August 2006), "The Grave Consequences of Supporting War in Lebanon", available at: *www.alternet.org/waroniraq*

- Vest, Jason (23 August 2002), "Turkey, Israel and the U.S", available at: *www.thenation.com*