JOURNAL FOR IRANIAN STUDIES

Specialized Studies

A Peer-Reviewed Biannual Periodical Journal

Year 4, Issue 12, October 2020

ISSUED BY

RASANAH
المعهد الدولي للدراسات الإيرانية
International Institute for Iranian Studies

THE ACTIVE FRONT: THE CONSEQUENCES OF CYBERWARFARE BETWEEN IRAN AND ISRAEL

Retired Major General Ahmed bin Ali al-Maymouni

A researcher on military and security affairs,
the International Institute for Iranian Studies (Rasanah)

ABSTRACT

The number of cyberspace attacks on key facilities has grown recently. The mutual cyberattacks between Iran on one side and Israel and the United States on the other have become something like a military phenomenon, which points to a new era of alternative military strategies instead of conventional military warfare. Between the ambitions of Iran in cyberspace and the capabilities of Israel backed by the United States, the conflict rages in the cyberspace sphere, becoming an invisible battleground, where the two parties fight to undermine each other's capabilities. It is part of the confrontation strategy between the two countries against the backdrop of mutual escalation between the two sides in regional operational arenas such as in Syria, Iraq, and other countries. Perhaps the intensity of the cyberspace conflict will increase, especially as it provides important advantages for both sides, such as avoiding a direct confrontation and the possibility of evading responsibility. In addition, the cost of launching cyberattacks is not high.

Introduction

Iran became increasingly aware of cyberspace's transnational capabilities and potential, especially after its nuclear facilities were targeted by a cyberattack in 2010,* and the confrontation with the opposition movement, which used online platforms to expand influence and place further pressure on the Iranian government. For example, the Green Movement in 2009 used Twitter to organize its activities. Therefore, Iran decided to engage in cyberspace battles to obtain knowledge and acquire technical capabilities through which it can protect its facilities against attacks and threaten its foes at home and overseas. On the other side, Israel, backed by the United States, possesses cyberspace capabilities. Therefore, it is capable of curbing Iran's ambitions to possess deterrent and offensive weapons.

According to some studies, *cyberwarfare** between Iran and Israel has expanded considerably to include the targeting of basic civilian infrastructure. Israel has so far managed to handle Iran's cyberattacks against its civilian infrastructure while suffering no severe damage. Nonetheless, it could be exposed to greater danger in the future amid the accelerating cyberspace armament race and Iran's acquisition of more complex capabilities.This is in addition to reports mentioning changes in Iran's cyberspace capabilities and its use of cheap programs to harm its foes and make other gains.

Other studies have touched on Iran's plan to rally national competencies in the sphere of cyberspace.This indicates that the scale of the conflict in cyberspace will expand further, and it will have important implications and will become a priority for Iran in the coming phase.

This study aims to clarify the impact of cyberspace on both Iran and Israel considering the current international situation which has witnessed growing tensions and polarization over the Iranian issue. In addition, this study reviews the cyberspace attacks in the aftermath of growing tensions between Iran and Israel and the extent to which cyberwarfare is effective as an alternative to conventional warfare through analyzing the capabilities of both countries in cyberspace; the mutual attacks; the mutual escalation in recent times; and the opportunities and challenges in this sphere.

I. Iran's Cyberspace: Objectives and Capabilities

Iran has sought to develop its capabilities to engage in electronic warfare and reconnaissance to neutralize the technical capabilities of its rivals in the region

(*) A cyberattack carried out by the United States and Israel on Iran's nuclear facilities to stop the production of uranium as part of Iran's nuclear program. Stuxnet Virus was used in this attack, a multi-part worm which spreads through the Windows operating system through USB sticks. It was developed in 2005 by the United States and Israel.

as well as the government's foes at home and overseas. Iran has taken advantage of low-cost technology and acquired new capabilities needed for espionage and sabotage.

Iran has adopted a strategy which has been in the pipeline for years. The strategy was designed, prepared, and developed in line with the ruling elite's vision and objectives. A technology expert mentioned when describing how far Iran is interested in developing its cyberspace capabilities, "Out of any country on the planet, I can't think of a country that has been more focused than Iran from the high levels of government on cyber, and that includes the United States."

According to this strategy, the IRGC and its surrogate, the Basij, lead the digital militias and battalions which are either linked with them or loyal to them in one way or another. They constitute a virtual force which was created in 2005 and named the Iranian Cyber Army. This virtual force is one of the digital arms used by the Iranian government to wage cyberattacks on its foes and opponents worldwide as well as on those countries opposed to Iran's nuclear and ballistic missile programs. It is also used in the field of intelligence and to gather information. Iran considers this field a new and active arena in its confrontation with the United States, its allies, and the government's opponents at home and abroad.

The Iranian cyber system includes trained personnel in the fields of information technology and hacking. It is regulated in accordance with an administrative system which is similar to the state's administrative structure. This system organizes and oversees the bodies and personnel in charge of Iran's cyberwarfare. The most prominent ones are as follows:

1. The Supreme Council of Cyberspace: It was formed in line with Supreme Leader Ali Khamenei's decree in 2012 and is composed of government officials from the main state apparatuses. It is chaired by the president of the republic. The council oversees all the bodies in charge of cyberspace and determines all policies in this sphere as well as the extent of the operations.

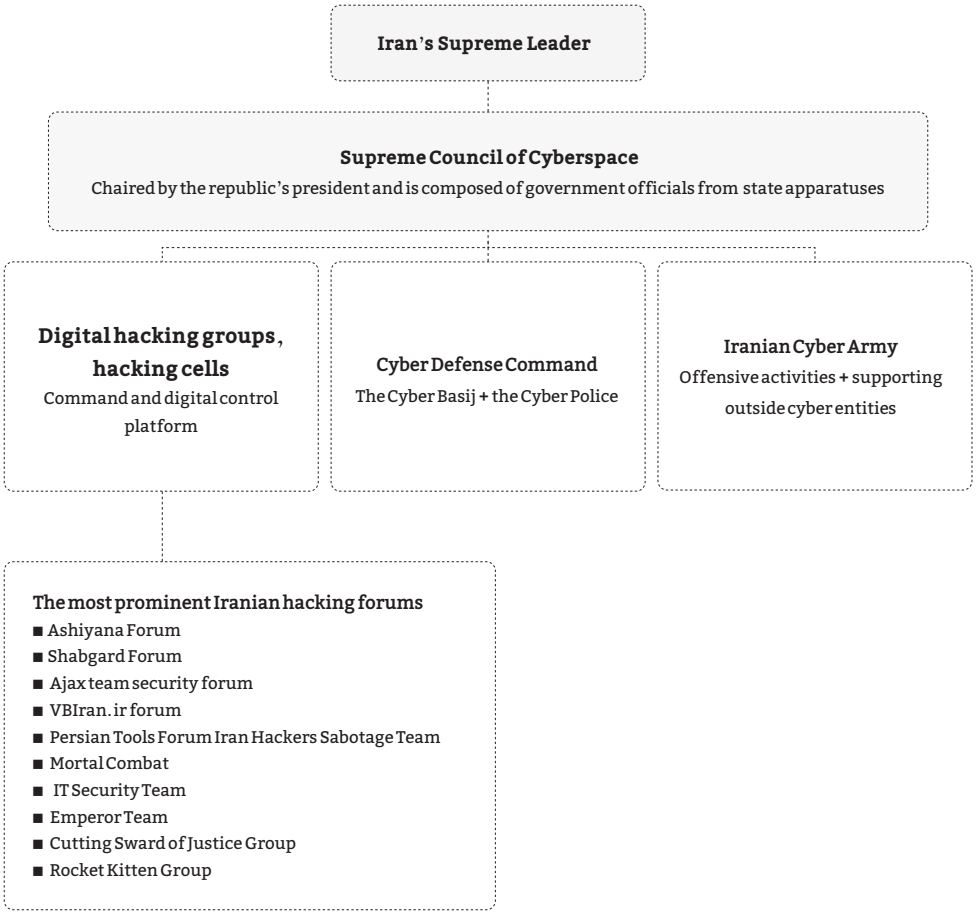
2. The Cyber Defense Command: The mission of this body is defensive. It protects national facilities from cyberattacks. It is linked to the Civil Defense Organization, which is part of Iran's Armed Forces.

3. The Iranian Cyber Army: Focuses on the offensive aspect of Iran's cyber force and is linked to the IRGC command/cyber force and includes high-caliber experts in the sphere of information technology as well as professional hackers to target Western media outlets, opponents, the interests of enemy countries and to gather information. A host of technical units support this offensive arm.

4. Supporting cyber hacking forums: Many cyber groups are working under the auspices of the Iranian government, which supports all the hackers existing in Iranian cyberspace. It has also recruited other hackers from outside the country who belong to loyalist organizations in Syria, Lebanon, and Yemen. The government also spearheaded the formation of a network of digital bodies to

achieve its political objectives in the region. These bodies threaten and engage in cyberattacks, cyber espionage and digital fraud to project the government's influence in the region.

Figure: Hierarchy of Iranian Cyberspace Capabilities



Source: prepared by the researcher.

Iran has allocated a significant percentage of its budget to develop its cyber capabilities. The Iranian cyber security budget rose between 2013-2017 by 1,200 percent. On this issue, Frank Cillufo, Director of the Center for Cyber and Homeland Security and the Vice President of George Washington University, said in 2017, "In recent years, Iran has invested heavily in building out their computer network attack and exploit capabilities. Iran's cyber budget had jumped twelvefold under President Rouhani, making it a top-five cyber power. They are also integrating cyber operations into their military strategy and doctrine."(1)

Iran's exertions in the cyber sphere include mobilizing national capabilities and taking advantage of this to serve government objectives. Iran has also used this sphere to spread misinformation about the source of attacks, thereby relieving the government of this task. Furthermore, the government allows Iranian hackers to freely access cyberspace, turning a blind eye to their hacking activities whether at the individual or group level. Hackers operate using different names, aliases, or the names of specialized companies. This operational tactic has contributed to Western study centers not possessing specific proofs about the nature of joint coalitions and policies. In addition, it has protected the Iranian government from direct accusations of preparing or carrying out cyberattacks against the websites of those countries that oppose its policies in the region. However, the Iranian government failed in hiding the suspects involved in cyber operations, particularly after the number of its digital hacking groups and teams increased. This failure was compounded by its formation of digital militias, recruiting digital proxies in the Arab region, the advanced level of their attacks, and the multiplicity of the bodies involved in preparing and carrying out attacks.[2]

To understand the effectiveness of Iran's cyber capabilities, without overstating existing capabilities, technical indicators highlight that current Iranian capabilities do not match Chinese cyber capabilities. The annual "2014 M-Trends Threat Report" from cybersecurity firm Mandiant reveals key insights on Chinese and Iranian cyber activities. It confirms that Iran-based threat actors (hackers) are limited to targeting certain sectors, particularly energy and government sectors. Meanwhile, in comparison, Chinese actors target more than 33 different sectors. In addition, the likelihood of detecting an Iranian hacker is 75 percent while for China it is 33 percent. Finally, the average timespan for detecting an Iranian hacker is 28 days while the duration extends to 243 days for a Chinese hacker.[3] Nonetheless, Iran is focusing its efforts to boost its capabilities in cyberspace and its offensive cyber activities indicate that Tehran is expanding its capabilities in this sphere.

Table 1 shows Iran's cybersecurity capabilities compared to some countries in the region, according to the Global Cybersecurity Index (GCI) 2018 which was formed by the International Telecommunication Union (ITU).[4]

Table 1: Global Ranking GCI 2018

Order	Country	Global Ranking
1	The United States	2
2	Saudi Arabia	13

Order	Country	Global Ranking
3	Turkey	20
4	Egypt	23
5	Israel *	39
6	Iran	60
7	Iraq	107

Source: *Global Cybersecurity Index (GCI) 2018*, International Telecommunication Union (ITU), https://bit.ly/3f5HWz7.

Israel considers that Iran is among the most active countries in the sphere of cyberspace, according to the claims of the Chairman of the Israeli National Cyber Directorate Yigal Unna. He has indicated that the Iranians have been working for a long time to carry out large-scale cyberattacks, including attacks to gather intelligence information and operations designed to cause extensive damage to systems. Iran is among the few countries that has carried out destructive cyber-attacks. Western experts have highlighted major spikes in Iranian cyber activities. According to a survey undertaken by Microsoft in March 2019, Iranian cyber groups during 2017 and 2018 mounted attacks on thousands of individuals and more than 200 firms around the world. The attacks caused huge losses worth millions of dollars.[5]

Also, Iran, via its cyber intelligence capabilities, can seize technical information which it can potentially harness to develop its different industries. It has already attempted to do this through operations targeting many university research centers in a number of countries.[6]

II. Israeli Cyber Objectives and Capabilities

Israel possesses advanced capabilities in the sphere of cyberwarfare, surpassing Iran's cyber capabilities. Israel is one of the major countries in the sphere of cyberwarfare.[7] Since the establishment of Israel's Military Intelligence Unit 8200 in 1948 by a cohort of elite Israeli computer engineers, which was tasked with gathering information and carrying out cyberattack operations, Israeli cyber efforts have covered different cyberspace aspects, including defensive/offensive attacks, espionage, gathering information and monitoring hostile activities on the internet.[8] After a spate of cyberattacks targeting several facilities in Israel, the Israeli government, in 2015, established a specialized cyber unit with offensive

(*) "The countries marked with an * are countries that did not participate in GCI 2018. They have neither submitted their answers to the questionnaire nor validated the data collected by the GCI team."

and defensive capabilities. This reflected a greater focus on the cyberspace sphere as one of Israel's major security fields. This was followed by Israel establishing the Israel National Cyber Directorate, which coordinates civilian and military cyber operations and has improved defensive and offensive planning capabilities in the cyber sphere. [9]

The Israeli National Cyber Security Authority (NCSA) was established in 2016 under the direct supervision of the Israeli prime minister's office. Its mission was to manage all defensive operations as well as to execute them at the national level, allowing a full and permanent defensive response to cyberattacks. This is in addition to identifying and evaluating the existing state of affairs (enemy threats), gathering and checking intelligence information, as well as working with concerned institutions to insulate them, particularly those linked to vital infrastructure, even if there is no state of war or looming danger.

The "IDF Strategy" document released in 2015, called for balanced defense in different circumstances and in all combat areas, including the cyber sphere, and supplying appropriate defense equipment to prevent hostile attacks. The document also pointed to using cyberspace to influence public opinion, develop international legitimacy, legal support and maintain media superiority after wars. With respect to the offensive aspect, the document called for securing capabilities to carry out preemptive cyberattacks. The offensive aspect surpasses the defensive one in the "IDF Strategy" document. Therefore, cyberattacks can be understood as a weapon used by Israel during wartime and peacetime alike. It is important to gather information and achieve some objectives via military operations that are consistent with Israel's security doctrine: deterrence, resolution, warning, and defense.[10]

III. The Reciprocal Cyberattacks Between Iran and Israel

From April 24-25, 2020, several facilities of Israel's Water Authority came under cyberattacks. According to the Israeli narrative, the attacks were handled by the NCSA. The report submitted by the chairman of the Water Authority to the head of the cyber department in Tel Aviv indicated that the facilities faced multiple cyberattacks, however, no damage was caused as a result thereof. The employees of the Water Authority were instructed to change the passwords of the main systems and to unplug some systems from the internet. In addition, Israeli officials pointed out that the attacks intended to take down the computer system which controlled the distribution of treated water, chlorine pumps and the chemicals used in treating sewage water. [11] According to a Fox News report, the Iranians had used US servers in the attack, and they launched attacks targeting northern and southern Israel. It remains unknown whether the attacks intended to seize control of operational systems or merely disrupt pumping operations.[12] But the Financial Times later published information which indicated that Iran sought via the cyberattacks to poison the Israeli population by increasing the level of chlorine in the water.[13]

As for the Israeli perspective on the incident's dimensions, former head of the Shin Bet security agency's Cyber Department Arik Barbing said that the Iranian cyberattacks point to a new security era, and that this incident represents a new kind of war between Iran and Israel — which could probably trigger a global war with dangerous consequences for the infrastructure of the targeted facilities. The former head of the Israeli Military Intelligence Directorate Amos Yadlin pointed out that the escalation in cyberattacks indicates that cyberwarfare has become a new military dimension along with the conventional ones: ground, naval and air warfare.[14] Israel also deemed this attack as a significant escalation by Iran, with Tehran crossing a red line.[15]

In what seemed to be a reprisal, Israel, on May 18, 2020, carried out a cyberattack targeting the Shahid Rajaee port terminal in the Strait of Hormuz. The attack disrupted the movement of navigation via the corridors and routes leading to the port. This was considered by some Israeli media outlets as Israel's revenge in response to the Iranian cyberattacks targeting the water distribution systems in rural areas of the country. A US government official, who declined to be named, told The Washington Post that the attack was highly precise and that the damage caused to the Iranian port was much more extensive than what was announced by the Head of the Iran Ports and Maritime Organization Mohammad Rastad. He told the Iranian news agency Eliba that the cyberattack did not hack the organization's computers, it only managed to hack and destroy a number of special operation systems.[16] However, Israeli reports indicated that the Iranian cyber defense mechanism Digital Fortress also known as the Dzhafa Project — which Iran claims is capable of protecting against cyberattacks and was developed in an independent country — was not effective, and was hacked repeatedly.[17] The head of the Institute for National Security Studies, Maj. Gen. (res.) Amos Yadlin tweeted, "If Israel was the one that responded to the Iranian attack against civilian infrastructure (water and sewage), Israel is making it clear that civilian systems ought to be left out of fighting."[18]

An expert told Ynet, the online outlet for the Yedioth Ahronot newspaper, that the malware used by the Iranians to target the water operation/distribution system was developed by one of the IRGC's offensive cyber units and that Israel decided to respond by striking Iran's civilian infrastructure and leaked the story to international media outlets.[19]

These mutual attacks were not the first of their kind between Iran on one side and the United States and Israel on the other. Over the past 10 years, several cyberattacks were carried out, and several were disclosed. Iran has targeted several countries having interests with the United States. Iran believes that using the cyber sphere allows it to carry out reprisal attacks and pose threats, according to MetaCompliance, a British magazine specializing in information security.[20]

Table 2 illustrates in chronological order the cyberattacks between Iran and its foes (the United States and Israel), which led to heightened rivalry in the sphere of cyberspace.

Table 2: The Most Prominent Cyberattacks Between Iran and the US and Israel[21]

SN	Incidents and actors	Month/year	Characteristics and consequences
1	A cyberattack on Iranian nuclear facilities to cease the production of uranium as part of Iran's nuclear program, by the United States and Israel.	November 2010	Virus Stuxnet was used in the attack. It was uploaded on a USB flash drive to access Iranian computer systems operating the production program. This led to the destruction of nearly 1,000 enrichment units. The attack led to the curbing of Iran's nuclear capabilities. This attack and its devastating impact were among the reasons which prompted Iran to develop its cyber capabilities. This is in addition to the influence of Iran's opponents who continued to support the protests of the Green Movement on social media platforms and used such platforms to unify their efforts. This helped strengthen the movement and pushed the government to improve its capabilities in the cyber sphere to counter opposition threats and undertake measures to control public access to the internet, especially during times of popular unrest. The government ushered in the development of a national internet project: the "halal internet" also known as Iran's National Information Network (SHOMA). The government also has worked to restrict people's access to VPN networks.
2	A spate of cyberattacks by a host of Iranian hackers.	2011-2013	These targeted 47 of the most important American banks and financial institutions such as Bank of America, JP Morgan, and others. They were targeted by a distributed denial of service (DDoS) attack; thousands of bank customers were unable to access their accounts. These institutions incurred huge financial losses and huge costs to repair the damage caused to their electronic systems.

SN	Incidents and actors	Month/year	Characteristics and consequences
3	Iranian hackers attempted to access the control system of a dam in a suburb of New York city.	2013	The hackers attempted to obtain operational control of the flood gates, but they were unable to because the dam had been disconnected for routine maintenance at the time of the attack.
4	An Iranian cyberattack on the system of Adelson's Las Vegas Sands Corp.	2014	This was in response to the head of the corporation calling for nuclear weapons to be used against Iran. The attack disrupted the corporation's information systems and resulted in customer data and information being seized.
5	An Iranian group carried out intensive cyberattacks on US universities and institutions.	2013-2017	These attacks targeted the systems of 144 US universities and scientific institutions. Up to 31 terabytes of documents and data were hacked. During this period, the Iranian group attacked the systems of 176 universities in 21 countries and mounted attacks on the systems of 47 companies inside and outside the United States. This is in addition to targeting several US official institutions, the UN, and other organizations.
6	A US cyberattack on Iranian computers and missile control and launching devices.	2019	A US cyberattack was carried out against Iranian missile launching and control systems, through exploiting a flaw in the heavily guarded network. According to US news outlets, the cyberattack was launched based on an order from President Trump in response to the downing of a US Global Hawk drone —which had penetrated Iranian airspace. The retaliatory cyberattack was also in response to the Iranian attack against oil tankers in the Gulf of Oman. The attack targeted the computers of Iran's control system which is used to launch missiles and a network monitoring vessels in the Strait of Hormuz, which the Americans describe as an espionage network.

SN	Incidents and actors	Month/year	Characteristics and consequences
7	Cyberattacks said to have been carried out by Iran on the Israeli water network	April 24, 2020	Several facilities linked to Israel's Water Authority came under cyber-attacks blamed on Iran. According to the Israeli narrative, the incident was handled by the Israeli cyber unit. The report submitted by the chairman of the Water Authority to the head of the cyber department in Tel Aviv indicated that the facilities came under multiple cyberattacks, and no damage was caused as a result thereof. The passwords of the main systems were changed, and some systems were disconnected from the internet. Israeli officials also pointed out that the attack intended to take down the computer systems which control the distribution of treated water, chlorine pumps and chemicals used to treat sewage water.
8	An Israeli cyberattack that targeted Iran's Port of Shahid Rajaee in the Strait of Hormuz	May 9, 2020	The attack disrupted the movement of navigation via the corridors and routes leading to the port, in what was considered by some Israeli media outlets to be a revenge attack in response to the Iranian cyberattacks on Israel's water distribution systems in rural areas of the country. A US government official, who declined to be named, told The Washington Post that the attack was highly precise and that the damage caused to the Iranian port was much more extensive than announced by the Head of the Iran Ports and Maritime Organization Mohammad Rastad. He told the Iranian news agency Eliba that the cyberattack did not hack the organization's computers, it only managed to hack and destroy a few operational systems. However, Israeli reports indicated that the Iranian cyber protection system called Digital Fortress, which Iran claims can protect it against cyberattacks and was developed in an independent country, was not effective, and was hacked repeatedly.

SN	Incidents and actors	Month/year	Characteristics and consequences
9	Cyberattacks on Iran's nuclear facilities in Natanz; suspected to be Israeli cyberattacks	June 30, 2020	A series of mysterious attacks targeted Iran's nuclear facilities in Natanz and military positions in Parchin. Many analysts believe that these were cyberattacks carried out by Israel. Neither of the two sides confirmed the nature of the attacks. But Iran acknowledged that they were subversive operations. Israeli and American statements hinted that they were cyberattacks intended to disrupt Iran's nuclear program.

Source: prepared by the researcher.

In light of Iranian attempts to obtain intelligence information and research materials, an IRGC-linked cyber organization called Ajax Team – or Rocket Kitten – was unveiled in 2014. It focuses on attacking several bodies and individuals to gather intelligence and steal important information. This is a guided and systematic organization which has targeted Israeli scientists, embassy staff, NATO leaders, government opponents, the Saudi royal family, US/ Israeli interests, and news websites.[22]

Recently, pro-Iran hackers attacked the US drug company Gilead which is leading research to find a vaccine to treat the coronavirus. Although, Alireza Miryousefi, the spokesman for Iran's mission to the UN, denied that Iran was linked to the attack, there are several reports highlighting Iran's attempts to secure information to treat the coronavirus. Iranian hackers, and other hacking groups, attempted to hack the systems of the World Health Organization in a bid to seize research material in relation to the coronavirus.[23]

IV. Consequences and Outcomes of the Cyber Confrontation Between Iran and Israel

Though the hacking attempts between the two sides (Israel and Iran) continue ceaselessly and sometimes covertly, their intensity increases in certain situations. The two parties would sometimes indirectly declare their involvement in the attacks for the sake of deterrence or to send a certain message to their foe. Some believe that the ongoing cyberwarfare is a shadow of the ongoing war between the two sides in Syria and that there is a relationship between the mutual cyberattacks between Iran and Israel and the ongoing conflicts in the region. Yet maybe Iran has intensified cyberattacks on targets in Israel due to Tehran's awareness of Israel's military strength outweighing its own. This provides Israel the upper hand

to intensify its air raids on the targets and militias aligned with Tehran in Syria.[24]

Iranian maneuvers and the application of pressure using all means possible are an attempt to send a message to the world that it is capable of confronting the United States and its allies, including Israel, and that it has the capability to act when it comes under pressure. Among the means Iran has at its disposal is the use of cyberspace to target its so-called enemies. When Iranian nuclear facilities and missiles faced cyberspace attacks by the Americans and Israelis, Iran mounted several cyberattacks on key facilities inside the United States and Israel.

The mutual attacks in cyberspace involve each side hurting the other without reaching the phase of direct military confrontation. Hence, we could say that the Iranian cyber strategy is intricately linked to its geopolitical interests and adapts according to these interests. This distinguishes Iran's cyber strategy. Iran works actively in cyberspace when it experiences pressure. It had attacked the interests of the United States in the aftermath of the economic sanctions imposed by the United States and following the killing of General Qassem Soleimani. It also mounted attacks on Israel in the aftermath of Israeli attacks on Iranian forces and Iran-aligned militias in Syria.

Hence, Iran's offensive operations in cyberspace increase in response to escalation in geopolitical and economic spheres.

Yet, Iran's inclination to boast about its accomplishments from time to time — particularly about its technological and military accomplishments and ability to launch cyberspace attacks — advances its leadership ambitions and ability to compete head-to-head with major world powers and confront enemies. It also empowers the government's popular incubators at home, eases domestic anger and deflects the attention of the Iranian street from internal challenges to other external challenges. Moreover, cyberattacks do not trigger military confrontation as it is difficult to prove the origin of the attack, thus it is near impossible to pin the blame on a certain country or countries.

Iran has gradually developed its cyber capabilities from merely simple to sophisticatedly complicated attacks. The early Iranian attacks were denial of services (DoS) attacks. Later, the Iranian hackers managed to launch DNS [hijacking] —DNS is short for domain name server [or system]. Recently, Iran stepped up to launch sophisticated attacks; it created *Shamoon*, data-wiping malware, which penetrates into a network of computers and wipes all of the computers that are on that network. However, "the holy grail of attacks are viruses that can get into industrial control systems, or what are called ICS," which Iranian hackers have not mastered yet.[25]

Iran is making diligent efforts to advance its capabilities in the sphere of cyberspace because it is aware of the weaknesses of countries at the time being in this field, the lack of any international mechanism or legislation regarding cybercrimes, the difficulty to prove the original source of cyberattacks and the

ease with which responsibility can be denied. Cyber systems have become critical for all aspects of life.

Nonetheless, there are challenges facing Iran. These include the recent attacks targeting its nuclear facilities in Natanz, and military facilities in Parchin as well as the emerging speculation designating these operations as cyberattacks. This sheds light on Iran's low cyber protection and defense capabilities despite spending large sums to strengthen this.

The small-scale cyberattacks on Israeli infrastructure reveal the huge gap between Iranian cyber capabilities compared to those of the United States and Israel, which are much more advanced. Israel has targeted key facilities inside Iran such as the country's nuclear program and the Port of Shahid Rajaee.

In view of the traditional defensive deterrence strategy adopted by Iran to forestall attacks on its soil and transfer the confrontation with adversaries beyond borders via investing in deploying aligned militias in a number of countries, the cyberattacks targeting key Iranian facilities puts the Iranian strategy of deterrence and forward defense into question. Cyberspace also makes it possible to mount attacks against key targets deep into Iran's territories, putting the future of Iranian defense in grave danger in case Iran comes under a direct attack. Iran has not developed its armed forces to allow them to counter all threats. This is Iran's concern, and it has long sought to prevent threats against its defensive depth in light of its fragile military system.

Also, Iran's limited technical capability to threaten well-protected networks makes it more vulnerable to cyberattacks. A good example here is the US attack targeting a software glitch in the network of an air defense unit linked to the IRGC, which was responsible for firing projectiles.

Israel, via the capabilities it possesses in the sphere of cyberwarfare, and the support it receives from the United States, can keep Iran under constant pressure. It can also curb any Iranian ambitions to win the race of military strength with itself. This is in order to prevent Iran from possessing any capabilities through which it can cross the redlines specified for it within the regional balances, particularly not allowing Iran to obtain nuclear or missile military capabilities which pose a threat to Israel. But Israel fears Iran's growing cyber capabilities, which can potentially become a source of threat to Israeli infrastructure, which depends on cyber technology.

As for Israel, it adopts a deterrent cyber policy against Iranian cyberattacks. This includes, for example, targeting the Port of Shahid Rajaee and its possible involvement in the suspected cyberattacks on Iran's nuclear facilities in Natanz to send a message that Israel's capability surpasses Iran's and that vital civilian facilities can be easily targeted and disrupted.

Therefore, it is possible that the cyberwarfare between the two sides will become more tense in light of the two parties attempting to add cyber deterrence to their other deterrence elements.

Nevertheless, some Israeli assessments suggest that cyberwarfare is still in its infancy, and therefore the confrontation in this sphere may escalate more and more in the future. It may extend to mounting attacks on civilian targets, as happened in the attack on the Israeli water network, which threatened Israeli lives. A cyberattack leading, for example, to two trains colliding with each other would be much more lethal than any ballistic missile. Of course, the current cyber confrontation increases the complexity of the security environment for Israel. Its rules differ from the rules of war known to date and geography has no importance in the cyberwar environment.[26]

This is in addition to the advanced cyber capabilities which could potentially fall into the hands of Iran-backed militias such as Hezbollah and Hamas.

In this respect, the author of "Inside Cyber Warfare" Jeffrey Carr believes that any country can mount a cyberwar on another country regardless of its software sources. This is because most military forces are linked to spying networks and connect to the internet. So, they are not secure. For the same reason, non-governmental groups and even individuals can mount cyberattacks and participate in cyberwars.[27]

It is worth noting that cyber risks are among the growing challenges threatening the global security environment and the global economy. These have been classified as among the 10 greatest risks facing the world.[28] This means that cyberwarfare will be a sphere of conflict and rivalry between Iran and Israel in the future. This is driven by their desire to possess this kind of deterrence and gain superiority over the other and is motivated by the investments they have been pumping into cyberwarfare technology for years.

Conclusion

Cyberwarfare, considering the advanced cyber environment, has become a new military reality and dimension through which states compete to inflict damage on foes in a way that does not drain resources and without human losses. It makes the control of the outcome possible, unlike conventional wars, which cannot always be ended. The cyber realities indicate that cyberspace has become a fertile environment for rivalry and that cyberwars will have a greater role in future conflicts. Cyberwars will play a role at the tactical level and will prevent the escalation to an all-out war.

A lot of countries are now developing their strategies in cyberspace to create a sense of relative deterrence in this sphere. This puts cyber threats on the map of basic future threats facing countries.

On the other side, the region's countries will not be immune to Iranian cyber sabotage. Iran seeks to find any flaws or weaknesses in protection systems through which it can infiltrate and disrupt the cyber environment in any vital sector. It aims to display its capabilities and target everyone linked to the United States and its allies, as was the case when Saudi Arabia's Aramco oil facilities were targeted by Iran.

Endnotes

(1) Gabi Siboni, Léa Abramski, and Gal Sapir, "Iran's Activity in Cyberspace: Identifying Patterns and Understanding the Strategy," *INSS*, March 1, 2020, accessed August 25, 2020, https://bit.ly/2VdIz29.
(2) Alrazu, *Iran's Software Piracy and Digital Militias,* 144.
(3) Mandiant, "2014 M-Trends Annual Threat Report: Beyond the Breach," *FireEye*, April 2014, 10, accessed November 30, 2020, https://bit.ly/37fetAQ.
(4) International Telecommunication Union (ITU), "Global Cybersecurity Index (GCI) 2018," July 28, 2020, accessed August 25, 2020, https://bit.ly/3f5HWz7.
(5) Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace."
(6) "Hackers Affiliated With Iran Have Attacked an American Company Developing Drug for Coronavirus,", *Haaretz,* May 9, 2020, accessed August 10, 2020, https://bit.ly/35eJJR1, [Hebrew].
(7) Saleh al-Naami and Nidal Mohammed Wad, "Israeli Readings of the Cyber Confrontation With Iran," *The New Arab,* May 20, 2020, accessed August 25, 2020, https://bit.ly/2ECWl9a, [Arabic].
(8) Fatima Hassan 'Itani, *Israeli Unit 8200 and its Role in Serving Israeli Espionage Technology* (Beirut: al-Zaytouna Center for Studies and Consultations, August 2010), 9, [Arabic].
(9) Basil Rizk, "Israel on the Cyber Front," *Metras,* July 23, 2019, accessed August 24, 2020, [Arabic], https://bit.ly/3aTVLQt.
(10) Ibid.
(11) Ahiya Raved, "Cyber-attack Targeted Israel's Water Supply**,** Internal Report Claims," *Ynet News,* April 24, 2020, accessed September 6, 2020, https://bit.ly/324oLlU.
(12) "Report: Iran Behind Hack of Israeli Water Authority Sites," *Ynet News,* May 7, 2020, accessed August 10, 2020, https://bit.ly/3mgS5gG.
(13) "Iran Tried to Poison Israelis by Increasing Chlorine in Water," *Ynet News*, June 10, 2020, accessed September, 6, 2020, https://bit.ly/36jnGsp.
(14) Amal Shehadeh, "A Cyberwar Between Israel and Iran Is No Less Dangerous Than the Military One," *The Independent Arabia,* May 20, 2020, accessed September 6, 2020, https://bit.ly/3jWJZbH, [Arabic].
(15) "Israel Discusses an Iranian Cyberattack Targeting Water Facilities," *Channel 13* (*Reshet 13*), May 9, 2020, accessed August 2, 2020, https://bit.ly/2DCMsbI, [Hebrew].
(16) " 'The Washington Post:' Israel Launched a Cyberattack on an Iranian Port," *The New Arab*, May 19, 2020, accessed September 06, 2020, https://bit.ly/320REiY[Arabic].
(17) "Cyber Strike Confirms to Iran: Infrastructure Is a Red Line," *Israel Defense,* May 20, 2020, accessed August 6, 2020, https://bit.ly/3lVzszi, [Hebrew].
(18) Amos Harel, "With Cyberattack on Iranian Port, Tehran Gets a Warning: Civilian Installations Are a Red Line," *Haaretz*, May 15, 2020, accessed August 10, 2020, https://bit.ly/3mz7zgp.
(19) "Host of Israeli Sites Targeted in Massive Cyberattack," *Ynet News,* May 21, 2020, accessed August 10, 2020, https://bit.ly/3mzbqtT.
(20) Geraldine Strawbridge, "Iran's Cyber Attack Timeline 2009 – 2020," *MetaCompliance*, January 21, 2020, accessed September 9, 2020, https://bit.ly/3he9rHA.
(21) Jehan Lotfi, "Cyberwarfare and US Cyber-attacks on Iran Missiles," *Spuntik Arabic*, June 25, 2019, accessed October 8, 2020, https://bit.ly/2I9vgwj, [Arabic]; Khaled al-Minshawi, "Why Is Iran Preparing to Repel Material or Cyberattacks Against Its Oil Installations?" *The Independent Arabia,* September 30, 2019, accessed October 8, 2020, https://bit.ly/34vCIcC [Arabic] ; and "Iranian Bombings Motives and Outcomes," *Fikr Center for Strategic Studies,* July 19 , 2020, accessed September 6, 2020, https://bit.ly/35nDfzB, [Arabic].
(22) Siboni, Abramski, and Sapir, "Iran's Activity in Cyberspace."
(23) "Hackers Affiliated With Iran Have Attacked an American Company Developing Drug for Coronavirus."
(24) Al-Naami and Wad, "Israeli Readings of the Cyber Confrontation With Iran."
(25) Sophie Bushwick, "How Iran Can Still Use Cyber and Drone Technology to Attack the United States," *Scientific America,* February 23, 2020, accessed August 12, 2020, https://bit.ly/3lChPnd.

(26) "The Cyber War Between Tehran and Tel Aviv Breaks out 'Officially!'" *180Post*, May 22, 2020, accessed August 24, 2020, https://bit.ly/2QnXrs0, [Arabic].
(27) Ramah al-Dalqamouni, "May Paralyze Entire Countries: Has Cyberwarfare Broken Out?" *al-Jazeera.net,* January 7, 2020, accessed September 9, 2020, https://bit.ly/3bF5wlY, [Arabic].
(28) "The Global Risks Report 2019-2020," *World Economic Forum Global Risks,* January 2020, accessed October 7, 2020, https://bit.ly/3iKAo6Q.