JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 37, 1273-1287 (2021)
DOI: 10.6688/JISE.202111_37(6).0003

Intelligent System for Measurement and Appreciate a Country Power, Capabilities

MOHAMMED ABU SAADA AND YILDIRIM TURAN
Middle East Institute
Sakarya University
Sakarya, 34000 Turkey
E-mail: abumo7719@gmail.com; yildirimturan@sakarya.edu.tr

The paper aims to shed light the would illustrate how much Iran has developed and promoted its cyber-war capabilities. The study has reached numerous findings, most notably the fact that soon after the provision of Internet in the capital Tehran in 1995, major Iranian universities started to play a key role in launching the nation's cyber security policy; teaching computer science students the basics of hacking, cyber security, and information security, which stimulated the Iranian National Security Council to form various Iranian institutions and external electronic agencies to act as Iranian offensive arms. Although Iran's cyber capabilities are weaker than those of Russia and China, it has become clear that Iran is an emerging cyber power that poses a real major threat to the United States and its allies. Iran's cyber-attacks primarily targeted Saudi Arabia, then they moved to Israel, and after that to the United States, Britain, Canada, and other Western countries. Later, Iran was subjected to fierce cyber-attacks by the United States and its allies, estimated at about 33 million attacks in 2019 alone. However, due to conflict of wills between Iran and the United States of America in the Persian Gulf and the Strait of Hormuz on the one hand, and between Iran and Israel on the other – on many regional files, most notably Iranian support for groups Israel classifies as terrorist organizations – the study suggests that cyber warfare is most likely to escalate between these parties within the coming period, in light of the low strategic costs of such confrontations.

Keywords: intelligent system for measurement, power, capabilities, intelligent appreciate,

1. INTRODUCTION

Senior decision-makers in Iran participate in all decisions related to cyber warfare through the nation's official security institutions such as the Ministry of Intelligence and Security (MOIS) and the Islamic Revolution Guard Corps (IRGC). Iran's official interest in cyber warfare comes upon directions from the Iranian Supreme Leader Ali Khamenei; who believes that electronic warfare is an important tool to amplify Iran's power and enhance its position internationally. It is noteworthy that several factors have motivated the Iranian supreme leader to adopt this approach, most notably:

a) Leveraging the power of the Internet as it represents a new source of power provided on an equal basis to most countries, especially in light of the continued international sanctions imposed on Iran, which resulted in a sharp deterioration in the Iranian economy and consequently affected its ability to extend its external influence.

Received September 2, 2020; revised September 6 & 23, October 2, 2020; accepted October 5, 2020.
Communicated by Amine Mohammed El Abdelli.

b) The Internet's ability to connect Iran with the outside world, which reduces its international isolation.
c) The limited total costs of cyber warfare, which are much lower than their traditional counterparts; for example, the cost of a cyber-attack may not amount to the cost of buying one tank, where a cyber-attack only needs some modern and advanced electronic weapons as well as human skills and creativity; while it does not require a commitment to time constraints or political circumstances, whether in time of peace, war or crises; as its implementation only requires a specific time. This led Richard Clarke, the chief White House advisor, to state that cyber warfare has emerged as the first security challenge in the 21st century.
d) Competition between major powers has motivated various countries to adopt aggressive policies. Russia, the United States, the NATO, North Korea, Iran, Israel, and other countries have all moved gradually from a defensive approach to an aggressive stance, which has increased their cyber activities, especially as cyber warfare is not bound by agreements and treaties. Besides, such warfare enjoys secrecy (anonymity and lack of engagement rules); therefore, the cyber domain has become extremely attractive to Iran, which is attempting to position itself as a major player on an equal footing with superpowers. In this regard, Behrouz Esbati, the commander of Iran's General Staff Cyber Headquarters (GSCH) summarized the Iranian interest in cyber security during an interview in 2015 with Defa Press, an Iranian media outlet, when he stated that "cyber security and capabilities are no less important than the nuclear issue". This comment outlines the high-level strategic significance that Tehran has given to the promotion of its ability to defend and attack through digital networks.

Based on Iran's official desire to develop the nation's electronic capabilities, this study aims at shedding light on the development and promotion of the cyber capabilities of Iran, one of the most closed countries all over the world by exploring the history of the Internet in Iran and addressing some Iranian external cyber-attacks, which would highlight how far Iran has come and promoted its capabilities in cyber warfare.

Therefore, the study addresses the history of information and communication technology in Iran, Iranian external cyber-attacks, and the most important cyber-attacks launched by external powers against Iran.

2. THEORETICAL RSSI MODEL

Some countries, such as the United States of America, had realized the importance of the Internet earlier than other countries, which made them more interested in the cyber activity and more successful in using it in military and civilian areas. However, some countries still look at technology in general and the Internet in particular as a byproduct, despite its international reach, which is mostly due to the extent of development, urbanization, and strength of these countries, along with the will and wit of their governments.

Given that Iran is one of the most influential regional countries in the Middle East, this article will attempt to shed light on the development of the Internet and information technology in Iran, as follows:

2.1 A Brief History of the Internet in Iran

Since 1993, Massoud Saffari, head of Iran's High Council of Informatics, had started working on a national activity to make a devoted data communications network utilizing the nation's current phone framework. A couple of years following the dispatch of this activity, Iran built up its first commercial Internet Service Provider (ISP) through working with the non-profit Neda Rayaneh Institute (NRI), which is a branch of the municipal government of Tehran. In February 1995, the recently made ISP started offering web access, principally in the capital Tehran. Around the same time, the Telecom Company of Iran (TCI), as a team with the state-controlled Telecom Infrastructure Company (TIC), conformed its its monopoly with the acquisition of international internet gateways in the nation and assumed control of single domestic ISP and internet providers.

It is to be mentioned that the TCI started its activity in the field of the Internet in Iran in 1994 when it announced the development of a nationwide packet-switched network called IranPac. However, the arena of the Internet in Iran in the 1990s was not restricted to the Iranian Telecom Company (TCI), but there were other operating companies, most prominently:

The Data Communication Company of Iran (DCI) is a public business entity that looked to assume control of IranPac after it started in 1996 and 1997 and build up worldwide associations between its developing domestic network backbone and the worldwide web systems; and it prevailed with regards to entering an association with a Canadian telecom company called Teleglobe, which is currently VSNL International Canada. Teleglobe worked with the Intelsat satellite organization to give Iran its novel devoted satellite uplink directly integrated with the IranPac framework. A while later, the DCI went into a joint endeavor with the Kuwaiti Ministry of Communications and the US-based Hughes Network Systems (HNS) to expand the geographic territory supported by a devoted internet and data transmission service inside Iran, and improving web speed across the country. The DCI expected to have 300,000 government clients on its system by 1998, with plans to permit general public to buy modems for personal use in that year. This target affected the internet in Iran; and by 2001, Tehran alone had 1,500 web cafes. Today, Iran has around 89 million users, and almost 30 million of them have access to 3rd or 4th generation mobile data services.

The Institute for Studies in Theoretical Physics and Mathematics (IPM) was established in 1989, as an institution affiliated with the Iranian Ministry of Science, Research, and Technology. However, it has become a semi-separate entity and with the same name since 1997. The Institute started its work with only three research groups in theoretical physics and three other research groups in mathematics. As for now, the institute is comprised of 9 schools researching many different areas of fundamental sciences, namely, School of Biological Sciences, School of Astronomy, School of Physics, School of Cognitive Sciences, School of Mathematics, School of Particles and Accelerators, School of Nano Science, School of Computer Science and School of Philosophy. The government has placed the Institute responsible for some national activities, most noticeably: the Iranian National Observatory and the Advanced National Computing Center.

The IPM was the first establishment in Iran that made the infrastructure crucial to get associated with global networking in 1992, and it bit by bit made this service accessible to other scholarly organizations. This network has advanced and changed into the current

Science-Research Network of Iran (Iranet) which works under its watch.

Iran has preferred a well-established national internet infrastructure that was gradually becoming easily accessible to most of the populace, even though the network transmission services were slower and fees of the same were restrictively exorbitant for the nation's low-income individuals. Be that as it may, the countrywide internet infrastructure and committed computer industry have been dynamic and established for at least thirty years. The presence of this telecommunication backbone and the developing commercial and private accessibility to the web after 1998 has brought about computer software and hardware literate population. In May 2009, in terms of Internet capabilities, the American Security company listed Iran among the most powerful five countries.

2.2 Cyber in Iran

Major Iranian universities are considered the cornerstone of Iran's interest in the field of cyber world. For instance, the Sharif University of Technology in Tehran has built up its committed Security and Counter-Infiltration training program where undergrad and graduate software engineering students are shown basics of hacking, cyber security, and data security policy. The educational program incorporates a prologue to operating systems; penetration tests for remote systems; Firewall frameworks; and Identifying security lapses for XSS in web-based software or applications.

Accordingly, Iranian universities have contributed to strengthening the role played by Iran in the arena of cyber capability. In 2013, Iran started a countrywide educational program accentuating scripting and hacking at the secondary school level. The courses conducted for secondary school students focused on hacking the computer systems that backed unmanned aerial vehicles (UAVs), where capable software engineering students are trained in remote access and authorization control techniques. A large number of these students are coordinated into cyber security and information assurance university programs in Tehran.

In 2007, the Islamic Revolutionary Guard Corps (IRGC) built up the Center for the Study of Organized Crime, to target foreign adversaries, which drove Intelligence and government authorities in the West to classify this Center as Iran's first government composed hacking group. In 2009, the IRGC started selecting experts for its internal cyber force and the connected military unit called the Iranian Cyber Army (ICA). Besides, IRGC Commander Hossein Hamedani reported in 2010 that the Basij Cyber Council – an extra cyber entity under the IRGC – had prepared 1,500 cyber security experts to be deployed as a major aspect of its developing offensive attack and espionage outfit.

In mid-2017, Iran has put funds in working out its computer network attack and exploit capabilities. Iran's cyber funds had grown twelvefold under President Hassan Rouhani, making it a top-five cyber-power. Iranians likewise incorporated cyber operations into their military procedure and tenet. This was the deterioration of security relations between Iran and many international and regional powers, particularly Israel.

Therefore, Iran has developed its national security strategy, relying on two main pillars:

1) To protect Iranian national security by building a scientific, technological, and intelligence infrastructure, which adapts a preventive strategy during defense and a pre-emptive strategy during the offense.

2) To develop many of its combat concepts and traditions by forming a complex network of electronic armies capable of launching multiple cyber-attacks against specific targets simultaneously. This is in addition to activating its intelligence capabilities in the dissemination of misinformation and abortion of anti-Iranian government protest rallies. To achieve these goals, Iran has recently established a sophisticated network of educational and research institutions, in addition to the role played by the Ministry of Communications and Information Technology and the Iranian Communications Research Center in various areas of advanced technology, including information security. Moreover, the position of Technology Cooperation officer associated with the Iranian President's Office has been created, establishing control of research projects in the field of information technology at the highest level in the Iranian government.

In addition, Iran uses complementary units that are somewhat less efficient than the Iranian central Internet units. Besides the Basij electronic army for internal operations, the Iranian National Security Council has created many electronic agencies that operate within the framework of the Supreme Council for Cyberspace, most prominently:

Table 1. Firas Elias, "The Doctrine of Cyber security in Iran and the equations of confrontation with America," Noon Post, August 14, 2019.

01	Cyber Defense Command	02	Iranian Cyber Army
03	Information Coordination Center	04	Qods Force Cyber Army (External Operations)
05	Syrian Electronic Army (SEA)	06	Izz al-Din al-Qassam Cyber Fighters
07	Saif Al-Adel Group	08	Hezbollah Electronic Army
09	Parastoo Electronic Group	10	Police Service (Internal Cyber Security)
11	Committee to Identify Unauthorized Internet Sites		

2.3 Iran's Cyber Capabilities

Despite the fact that Iran's cyber capacities are viewed as weaker than those of Russia and China, unmistakably Iran is developing as a gigantic cyber threat to the United States and its allies. The Iranian cyber potential can be better clarified by General Moharam Gholizadeh, the deputy for electronic warfare of the Iranian Islamic Revolutionary Guard Corps (IRGC), who asserts that Iran has technological capacities that far surpass the ability to hack into the GPS of a drone and even capacity to change the course of a GPS-guided missile. Iranian authorities have concentrated on the cyberspace as an essential flashpoint in their regime's unfurling encounter with the West. Thus, the Iranian system has poured funds in its offensive cyber world. Late 2011, Iranian investments were assessed at more than $1 billion in the improvement of the nation's cyber capabilities. Although both the United States and Israel consider Iran an emerging player in the international cyber arena, they are much concerned that Tehran has received significant inputs to its strategic programs from China, Russia, and North Korea, given that such assistance has furthered its nuclear and ballistic missile capabilities. It is noteworthy that most of the Iranian cyber operations are carried out by the Cyber Defense Command, an organization established in November 2010 and operating under the supervision of the Passive Civil Defense Organization and which works under the superision of the Preventive Defense Organization, which is itself a subdivision of the Joint Staff of Iranian Armed Forces.

It is important to note that Iran's cyber capacities were less evolved during the period of 2012 and 2014, so its assaults were regularly one-off occasions instead of continued crusades. In any case, today Tehran follows the case of China, Russia, and the United States of America, continuing long-term reconnaissance and espionage operations that give access and intelligence. For instance, security firms and the U.S. government have distinguished Iranian cyber-espionage activities focusing on U.S. government entities, critical infrastructure, military/commercial avionics, manufacturing, and engineering, among different sectors. Iranian hackers have supposedly focused on the Internet's domain name framework and siphoned information from Internet service providers and telecommunication organizations that could facilitate future activities.

According to some American reports published in 2012, Iran has become a highly developed state in the field of cyberspace, indicating that Tehran succeeded in December 2012 to launch Mehr, a home-grown alternative to YouTube that features government-approved video content designed specifically for domestic audiences. Also, reportedly, Iran has been working since 2009 on new software suites designed to better control social-networking sites.

The Iranian authorities likewise have expanded control of the domestic phone, mobile, and Internet communications through installing a sophisticated Chinese-origin surveillance system. Iran has got the Cyber Police, a dedicated division of the country's national police that was established in January 2011 to monitor activists who utilize the World-Wide Web. The Iranian system additionally has built up another government agency to screen the cyberspace; where the Supreme Council on Cyberspace was officially initiated by Iranian Supreme Leader Ali Khamenei in April of 2012, to fill in as an organizing body for Iran's domestic and international cyber policies.

It should be noted that, despite Iran's early awareness of the importance of cyber technology, it still faces many technical challenges, most prominently "data" – as information is considered as the most significant resource over the past 15 years, and it will most likely remain so for years to come, particularly how to transfer, move, store and manage data and how to make the most use of it – and ways to monitor and process the internet related to human life, to achieve the so-called "private internet". It should also be noted that these challenges are not limited to Iran only, but they are shared by many countries, including Israel.

3. CYBER-ATTACK CARRIED OUT BY IRAN

The Iranian cyber-attacks against the United States and European countries were not the beginning of cyber warfare. India and Pakistan have used cyber-attacks against each other since 1998. In 2000, cyber-attacks were also used in the conflict between Turkey and Armenia. By 2005, the Lebanese Hezbollah Army launched cyber-attacks against Israel. In the same year, cyber-attacks broke out between Indonesia and Malaysia. In 2007, Russia launched cyber-attacks on Estonia and Lithuania. In 2008, Russia attacked Georgia. However, cyber warfare has recently been favorable to Iran as a weapon for dealing with domestic and foreign opponents.

Following are some key Iranian cyber-attacks:

3.1 Iranian International Cyber Attacks

United States:

In 2011, Iran emerged as a threat to US cyber security after an Iranian engineer specialized in electronic warfare succeeded in landing a US drone in Iran, where the engineer reconfigured the drone's GPS coordinates to make it land in Iran at what the drone thought was its actual home base in Afghanistan. This 2011 incident revealed Iran's technological prowess internationally, which made the US Secretary of Defense, Leon Panetta, state that Iran's capabilities to shoot down drones would undermine US efforts to search for Iranian nuclear activities. To address these growing concerns, the U.S. Air Force concluded two contracts, worth $47 million, for developing a new communications system to replace GPS on aircraft and missiles.

Between 2012 and 2013, Iran launched Operation Ababil campaign against U.S. financial institutions through a group known as Izz al-Din al-Qassam Cyber Fighters. In 2013, the Syrian Cyber Army hacking group hacked the Associated Press Twitter account, reading "Breaking: Two explosions in the White House and Barack Obama is injured". The accident immediately affected the US stock market negatively. The Dow Jones Industrial Average DJIA, +2.99% immediately plunged and the S&P 500 SPX, +2.67% was reported to have lost $136.5 billion in market cap.

- In February 2014, Iran used the Shamoon virus in targeting the Las Vegas Sands Corporation, one of the most important and largest tourist and recreational institutions in the United States, hiring approximately 51,000 people. The Iranian cyberattack came in response to a statement by Sheldon Adelson (CEO of Las Vegas Sands), calling the United States to strike Iran with an atomic bomb.
- In March 2018, Iranian hackers launched a SamSam ransomware attack to cripple Atlanta's city government.
- On April 8, 2018, the Izz ad-Din al-Qassam Cyber Fighters and the Syrian Electronic Army launched attacks inside the United States in response to American attacks on Iranian electronic websites carried out on April 7, 2018.
- In May 2018, a day after President Trump's withdrawal from the JCPOA nuclear deal, cybersecurity firm CrowdStrike warned its clients about a "notable" increase in Iranian phishing activity. Less than twenty-four hours after the announcement of the US withdrawal from the nuclear deal with Iran, Iran attacked many websites in the United States, which indicates the development of Iranian capabilities in terms of rapid response for timing.
- In 2018, a private Iranian group called Charming Kitten was responsible for man-in-the-browser assault utilizing a browser exploitation framework (BEF) against different Jewish news outlets inside the United States that bolstered Israel. Similar assaults have likewise happened against the American Israel Public Affairs Committee (AIPAC), Jewish political and scholastic pioneers the world over, and associations supportive of Israeli activities in Gaza and Lebanon.
- On 20 June 2019, Iranian forces shot down a US Navy Global Hawk drone, costing about $240 million after it had been hit by a surface-to-air missile fired by the Iranian Revolutionary Guard's air defense unit.

The Iranian cyber-attacks against the United States are often considered effective. The US Department of Homeland Security issued a statement warning the American private sector that Iranian cyber activity is increasing and that Tehran could launch destructive hacking campaigns against sensitive U.S. infrastructure in case of increased tensions.

European Union countries:

Unlike the United States of America, it seems that the European Union countries were not exposed to massive cyber-attacks by Iran, due to many reasons, including the lack of Iranian-European differences compared to those between Iran and the United States. However, key Iranian attacks on EU countries include:

- On June 23, 2017, The Times British newspaper reported that Iran was behind a major cyberattack, where some 9,000 email accounts of MPs, including those belonging to Theresa May and other cabinet ministers, were subjected to a sustained attack. Therefore, the British government asked MPs and ministers not to use their official mails at that time.
- In 2018, Germany revealed increasing Iranian threats, where Iranian cyber-attacks were doubling, mainly targeting ministries and government companies, including the defense, space, and energy sectors.

The People's Republic of China:

- In January 2010, a hacking group called "Iranian Internet Army" attacked "Baidu", a famous Chinese search engine, where the search engine users were directed to a web page that showed a specific Iranian political message.
- In October 2010, the Iranian Cyber Army also carried out a cyber-attack on Twitter in the People's Republic of China.

3.2 Iran's Regional Cyber Attacks

Israel

The main Iranian cyber actors, such as the Ministry of Intelligence and the Basij Cyber Council demonstrated a relatively high degree of sophistication during Iran's attacks against Israel. In this regard, Iran has adopted a strategy of actively searching for vulnerabilities within Israeli infrastructure, corporate, and military information systems to enable exploitation during peace and wartime. Iranian cyberattacks against Israel have often been active in espionage, where some attacks coincided with the Israeli military incursions in both Gaza and Lebanon. Iranian cyber-attacks have targeted Israeli economic and military institutions, as well as Israeli infrastructure due to its heavy reliance on digital systems and networks for the transmission of information. This was mentioned by Israeli Prime Minister Benjamin Netanyahu in a statement in 2013, saying that Iran had begun targeting water, power, and financial transaction infrastructure, in addition to social service websites operated by the Israeli government.

Key Iranian cyber-attacks against Israel include:

- In 1999, electronic groups linked with the Palestinian Hamas movement attacked Israeli websites with the help of Iranian technology.
- In January 2009, the Israeli Internet infrastructure was exposed to a cyberattack, in

coincidence with the Israeli military attack on the Gaza Strip. The cyberattack, which focused on the websites of the Israeli government, was implemented by an estimated five million computers. This cyberattack is believed to have been carried out by an organization based in one of the former Soviet states.

- Post 2010, Iran, in collaboration with Hamas and Hezbollah hacking groups, directed Computer Network Attack (CNA) and Computer Network Exploitation (CNE) activities against the Likud and Kadima Political Parties, Israeli Security Agency (Shin Bet), the Office of the Prime Minister, the Defense Ministry, Home Front Command, El Al Airlines (Israel's national aircraft), Bank of Jerusalem, and operational segments of the IDF. During the assault, one of Hamas' transcendent hackers, Maagad Ben Juwad Oydeh, effectively penetrated IDF information communications network and routed data downlinks from IDF drones flying over Gaza to Hamas commandants, as per a Jerusalem Post article. By 2015, Oydeh had the option to extricate the global positioning system (GPS) signals from the drones he was focusing on, which permitted senior Hamas fighters to move forces and weapons away from monitored territories. Oydeh was captured in 2016 on charges of spying, conspiracy, contact with enemy agents, and participation in an illicit organization. In 2012, Israel faced a sophisticated cyber campaign that targeted Israeli military and political activities during its war on Gaza.
- In 2014, during the Israeli war on Gaza, Iran broke into the civil and military communications network in Israel, and the IDF's homeland security division encountered an temporary data framework breach when the Syrian Electronic Army – an Iranian-connected hacking group – compromised the IDF's website and briefly upload political messages slandering Israeli activities.
- In mid-2015, Iran directed effective spear-phishing and domain name system (DNS) spoofing assaults against different law offices, banks, and third-party IT vendors that serve the financial industry in Israel. In spite of the fact that the metrics of these assaults and the financial expenses are incredibly ambiguous and underreported, Israeli media and government proclamations show that specific assaults have compromised critical payment card industry (PCI), market trading, and index reporting information systems.
- From 2013 to 2015, Israeli-based Check Point Software Technologies attributed a series of corporate and government breaches across Israel's defense sector to Iran's regional allies, specifically the Hezbollah Cyber Army (HCA) that carried out a series of penetrations against companies and government sectors of the Israeli Ministry of Defense.
- In 2018, Iran targeted Israeli universities, banks, and commercial companies and incurred them major losses.
- In March 2019, Iranian hackers targeted the phone of the IDF Chief of General Staff, and Benny Gantz, the current head of the Blue and White party, reportedly had their phones hacked by Iranian intelligence. Israeli security companies also accused Iran of attempting to influence the elections that took place in Israel during that period.

Gulf countries

Norman Roule, who served as the US National Intelligence Manager for Iran (NIM-I) at the Office of the Director of National Intelligence from November 2008 until September 2017, said. “Iran has launched waves of cyber-attacks on the infrastructure of the Gulf states.” This statement came after Iran targeted its regional rivals in the Persian Gulf for years with cyber-attacks, whether for espionage or sabotage. Iran used to launch cyber-attacks on its neighbors in the Gulf and the Middle East, most prominently:

- In 2012, Iran suspended the work of the natural gas company "RasGas" in Qatar and deleted data from the computer of Aramco National Oil Company in the Kingdom of Saudi Arabia, an attack that was described as devastating. Iran's cyberattack depended on a powerful virus known as "Shamoon". At the point when seventy five percent of the computers of Saudi Arabia's Aramco state oil company were focused by Shamoon virus, the malicious software set off a program that supplanted Aramco's corporate data with an image of a flamed American banner at a predetermined time.
- In August 2017, a cyberattack linked to Iran caused an explosion at a Saudi petrochemical plant.
- In the first half of 2019, a spokesman for the Bahraini Ministry of Interior stated that "The Information and E-Government Authority in the Kingdom of Bahrain have intercepted more than 6 million attacks and more than 830,000 malicious e-mails."
- In July 2019, Iranian hackers targeted vital infrastructure and government computers in Bahrain. The Bahraini authorities detected hacking activities targeting its Electricity and Water Authority. The hackers shut down several systems, while the Bahraini authorities believe it is an Iranian test to prove its ability to disrupt the Kingdom of Bahrain. Also, according to some circulated reports, Iran has most likely targeted Aluminum Bahrain (Alba), one of the largest industrial companies in the Middle East and one of the largest aluminum producers in the world, with a cyberattack. Mostly, Iran targets the Kingdom of Bahrain for several reasons, most prominently the fact that it is a permanent home to the Fifth Fleet of the US Navy and that it is a close ally of the Kingdom of Saudi Arabia, which is Iran's regional rival.
- In August 2019, Iranian hackers targeted the systems of the Bahrain National Security Agency, in addition to the Ministry of Interior and the Office of the First Deputy Prime Minister.

Generally, Iranian regional cyber-attacks have forced Saudi Arabia and the United Arab Emirates to spend tens of millions of dollars to bolster their cyber defenses and defend themselves against any likely Iranian penetrations.

Massive attacks:

In 2013 and 2014, Iran was conducting major cyber operations that caused significant financial damage to companies across the West and the Middle East, including the United States, Canada, Britain, Israel, Saudi Arabia, and Turkey. In 2018, Iran targeted research institutes, universities, and professors all over the world, where it captured more than fifteen billion pages from databases and information assets for facilities in nearly twenty countries in violation of intellectual property rights. Security companies estimate the value of this intellectual property at $3.4 billion. Leaked documents in May 2019 revealed Iranian cyber-attacks carried out by an Iranian hacking group, Rana, reportedly working for the Iranian Ministry of Intelligence and Security, where the group attacked more than 200 targets in dozens of countries from Asia, Africa, Europe, and America, including aviation sectors, telecommunications, government bodies, and information technology sectors. FireEye, a US cybersecurity firm, first revealed that an Iranian hacking group, affiliated to the Iranian Revolutionary Guards' Basij unit and the Ministry of Intelligence and Security -APT33- was responsible for an array of breaches across infrastructure, banking, aerospace, and petrochemical industries in Israel, the United States, the United Kingdom, South Korea, and Saudi Arabia. Some of these attacks led to the disruption and destruction of Israeli information systems. Even Microsoft Corporation has not escaped Iranian cyber-attacks, where in March 2019, Microsoft announced that it was subjected to Iranian cyber-attacks that targeted more than 200 of its branches in the past two years.

This article will be complemented by the quantitative assessment conducted by ClearSky of cybersecurity about Iranian cyber-attacks. The assessment concluded that Israel was subjected to 14% of the total Iranian cyber-attacks, as the second most targeted country after Saudi Arabia, which came first – while the United States, Britain, Canada, and other Western countries were exposed to less than 3%. These figures confirm that Iran's offensive strategy has multiple goals and objectives and those Israeli information systems were among the most targeted regional electronic systems by Iran's cyber-attacks.

4. PERFORMANCE EVALUATION

Since 2006, the United States of America has intensified its cyber operations against Iranian government computer systems. However, the preparation for the largest US cyber-attacks started with the summer of 2009, when the George W. Bush administration decided to fund projects described as classified with an amount of $300 million to target Iran's nuclear program, where much of the funding was earmarked for US cyber-attacks against Iran as a priority.

Therefore, this article will address some of the cyber-attacks against Iran from major international and regional powers, as follows:

- In 2010, Iran suffered a severe cyber blow after Israel and the United States launched a malware targeting Iran's nuclear program. The computer virus was known as Stuxnet to affect Windows operating systems and industrial control programs manufactured by Siemens. The virus also spread through commercial and governmental information systems (IS) and peripheral devices that were important points within the supervisory control and data acquisition (SCADA) systems in Iranian nuclear production facilities. It is known that SCADA directly interacts with extremely important devices such as motors, sensors, alarms, pumps, valves, and other vital infrastructure, and Stuxnet has succeeded in destroying 984 centrifuges and other machines that Iran was using to enrich uranium for use in the nuclear weapons industry, including 100 centrifuges in Natanz alone, which disrupted Iran's uranium enrichment program. Stuxnet enabled both the United States and Israel to access "authorization certificates," and highly protected codes that operate Siemens industrial and interior computers in Iran. An Iranian technical study early 2012 concluded that the Stuxnet attack had hindered Iran's centrifuge program for nearly a year.
- In April 2011, Iran detected an American computer virus dubbed "Stars" that was designed to infiltrate and destroy its nuclear facilities. Also, in the same month, the Iranian Ministry of Oil came under electronic attacks through an electronic virus nicknamed "Wiper" coming from the United States, which led to the closure of several oil stations in Iran.

- In May 2012, the Iranian nuclear program was further attacked by a virus dubbed "Flame", which infected many government systems.
- In June 2012, the United States and Israel deployed the "Flame" virus to collect intelligence information on Iranian computer networks in preparation for a cyber warfare campaign.
- On April 7, 2018, the United States launched cyber-attacks on several Iranian websites.
- In June 2018, Washington launched a cyberattack on Iran, destroying a database used by Iran's Islamic Revolution Guard Corps (IRGC) in "attacking oil tankers" in the Persian Gulf, according to US officials.
- In 2019, the United States launched a digital penetration of the Iranian missile systems, in the exploitation of what it referred to as a flaw in the Iranian network, which it described as a "heavily guarded" network. This cyberattack targeted – according to official sources from the US Defense Department – crippling the Iranian Revolutionary Guard's air defense units. The United States justified the attack as a response to shooting down its sophisticated drone, Global Hawk.
- In the same year 2019, a Saudi group launched a cyberattack on the website of the Iranian Statistical Center for a short period. The hackers left a picture of the late Iraqi President Saddam Hussein on the website's homepage. This group is likely to be linked to groups with Baathist orientations. Those hackers that claimed responsibility for the attack, had called themselves "Daes", likening themselves to the "Daesh" terrorist organization.
- In June 2019, the US Cyber Command, in coordination with the Central Command in the Middle East, launched cyber-attacks against computer systems of an Iranian Intelligence Group targeting controlling Iranian missile launch systems.
- In September 2019, the U.S. launched a cyberattack against an unspecified number of Iranian agencies related to propaganda dissemination.
- In December 2019, Iranian Minister of Communications and Information Technology Mohammad-Javad Azari-Jahromi announced that Iran was exposed to a massive cyberattack, without revealing more details. However, he said that the attack was identified and repelled by the National Information Network Security Shield, known as Djafa or Dezhfa, and they are exploring its dimensions, explaining that the attack was extremely massive, and its dimensions must be checked carefully.
- In February 2020, Iran was exposed to cyber-attacks that targeted the celebrations marking the 41st anniversary of the Islamic revolution, along with an attempt to influence the results of the parliamentary elections in Iran, after disabling links to some internet providers for more than an hour.

Remarkably, most of the cyber-attacks in Iran were launched by the United States; therefore, the study suggests that it is due to the US administration's desire to lead the scene of conflict with Iran during this period to rid its allies of any likely risks, given the geographical proximity of US allies with Iran may transfer the cyber warfare to a conventional war, which is mostly rejected by Washington.

We conclude this chapter by referring to a statement by the Iranian Minister of Communications and Information Technology, Azari-Jahromi at the Munich Security Conference that was held in the Qatari capital, Doha in October 2019, stating that Iran's DEZHFA foiled 33 million cyber-attacks in 2019 Therefore, most of the above-mentioned cyber-attacks, as well as other declared computer attacks, represent only a small number of the cyber-attacks that Iran has been subjected to.

Accordingly, the Iranian authorities have become extremely cautious in dealing with any international missions that visit Iran, which may explain the comments of the International Atomic Energy Agency (IAEA) inspectors that Iranians distrust them, especially after Iran had been exposed to various cyber-attacks targeting its nuclear activity. This makes it difficult to accurately estimate the losses caused by cyber-attacks launched against Iran. Also, Iran's cyber institutions were targeted as well. In 2012, the US administration-imposed sanctions on the Iranian Ministry of Intelligence and Security, one of two organizations responsible for carrying out covert activities outside Iran, after accusing it of providing support to groups the US administration had classified as terrorist organizations, in addition to accusations of committing human rights violations. Also, the European Union in 2019 designated the Directorate for Internal Security of the Iranian Ministry for Intelligence and Security as a terrorist organization, due to involvement in violent and terrorist activity in Europe. Iran's Ministry of Intelligence and Security is known for using cyber intelligence capabilities, including offensive cyber measures, to achieve its goals. In addition, Israel's Mossad conducts proxy cyber-attacks against Iran through the use of the People's Mojahedin Organization of Iran (PMOI).

5. CONCLUSIONS

In this paper, it seems that the digital and electronic world will become a major component in the future of wars between nations, because of its extremely strong and influential results, especially since the electronic war does not require a national State or oil resources.

However, due to the escalating pattern of the conflict of wills between Iran and the United States in the Persian Gulf and the Strait of Hormuz; and Iran and Israel on many regional files, most notably Iranian support for Palestinian and Lebanese groups that Israel classifies as a terrorist, in addition to the Iranian-Saudi competition in many regional files, most prominently the Yemeni file – given that these regional powers are interested in developing their cyber capabilities – it can be said that cyber warfare is most likely to escalate between them within the coming period, considering that all parties prefer to engage in conflicts of this kind because of the low strategic costs of such confrontation. Therefore, cyber-attacks on digital financial systems and infrastructure installations such as power plants, railways, communication lines, and dams are expected to increase in the future, whether in Iran, Israel, the United States of America, or one of its Western allies. Although Iran's capabilities on cyber warfare and espionage are less significant compared to those of countries such as the United States, Israel, Russia, or China; however, its cyber capabilities are evolving. Despite the severe international sanctions imposed on Iran and the fact that it lives in a geographical hot spot politically and militarily, this did not discourage it from being one of the most significant countries over the world in the development of its cyber warfare capabilities.

REFERENCES

1. S. Cohen, "Iranian cyber capabilities: Assessing the threat to Israeli financial and security interests," *Cyber*, *Intelligence*, *and Security*, Vol. 3, 2019, pp. 71-94.

2. N. Caplan, “Cyber war: The challenge to national security,” *Global Security Studies*, Vol. 4, 2013, pp. 93-115.
3. F. Elias, “The doctrine of cyber security in Iran and the equations of confrontation with America,” *Noon Post*, Vol. ___, 2019, pp. _____.
4. Y. Unna, “National cyber security in Israel,” *Cyber*, *Intelligence*, *and Security*, Vol. 3, 2019, pp. 167-173.
5. E. Tikk, “Ten rules for cyber security, survival,” *Global Politics and Strategy*, Vol. 53, 2011, pp. 119-132.
6. L. Gundert, S. Chohan, and G. Lesnewich, “Iran’s hacker hierarchy exposed,” *Recorded Future*, Vol. ___, 2018, pp. ____.
7. A. Hanna, “The invisible U.S.-Iran cyber war,” United States Institute of Peace, 2019.
8. M. Landler and T. Abandons, “Iran nuclear deal he long scorned,” *The New York Times*, 2018.
9. A. Sami, “Bahrain undergoes severe cyber-attacks amid escalating tensions with Iran,” *Aram News Agency*, 2019.
10. B. Alhayani and H. Ilhan, “Image transmission over decode and forward based cooperative wireless multimedia sensor networks for Rayleigh fading channels in medical internet of things (MIoT) for remote health-care and health communication monitoring,” *Journal of Medical Imaging and Health Informatics*, Vol. 10, 2020, pp. 160-168.
11. B. Alhayani and H. Ilhan, “Efficient cooperative imge transmission in one-way mult-hop sensor network,” *International Journal of Electrical Engineering Education*, Vol. 57, 2020, pp. 321-339.
12. B. Alhayani and A. A. Abdallah, “Manufacturing intelligent corvus corone module for a secured two way image transmission under WSN,” *Engineering Computations*, Vol. 37, 2020, pp. 1-17.
13. B. Alhayani and H. Ilhan, “Hyper spectral image classification using dimensionality reduction techniques,” *International Journal of Innovative Research in Electrical*, *Electronics*, *Instrumentation and Control Engineering*, Vol. 5, 2017, pp. 71-74.
14. B. Alhayani and M. Rane, “Face recognition system by image processing” *International Journal of Electronics and Communication Engineering and Technology*, Vol. 5, 2014, pp. 80-90.
15. B. Al-Hayani and H. Ilhan, “Visual sensor intelligent module based image transmission in industrial manufacturing for monitoring and manipulation problems,” *Journal of Intelligent Manufacturing*, Vol. 4, 2020, pp. 1-14.
16. O. I. Khalaf and G. M. Abdulsahib, “Frequency estimation by the method of minimum mean squared error and P-value distributed in the wireless sensor network,” *Journal of Information Science and Engineering*, Vol. 35, 2019, pp. 1099-1112.
17. O. I. Khalaf, G. M. Abdulsahib, H. D. Kasmaei, and K. A. Ogudo, “A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications,” *International Journal of e-Collaboration*, Vol. 16, 2020, pp. ____.
18. O. I. Khalaf, G. M. Abdulsahib, and B. M. Sabbar, “Optimization of wireless sensor network coverage using the bee algorithm,” *Journal of Information Science and Engineering*, Vol. 36, 2020, pp. 377-386.
19. O. I. Khalaf and B. M. Sabbar, “An overview on wireless sensor networks and finding optimal location of nodes,” *Periodicals of Engineering and Natural Sciences*, Vol. 7, 2019, pp. 1096-1101.

Photo

Mohammed Abu Saada received the master's degree from Al-Azhar University in Palestine at the Institute for Middle East Studies. Now he is a Ph.D. candidate, Middle East Institute, Sakarya University, Sakarya, Turkey.

Photo

Yildirim Turan is an Assistant Professor of International Relations. He received his Ph.D. from Sakarya University. His main research areas are Middle Eastern Politics, Democratization in the Middle East and war studies. His recent works have been published in Turkish Journal of Middle Eastern Studies.