Saada, M. A., Turan, Y. (2021). "Israeli-Palestinian Cyber Conflict", Eskişehir Osmangazi Üniversitesi İİBF Dergisi, 16(1), 186 – 204.
Doi: 10.17153/oguiibf.869178

Başvuru: 27.01.2021 *Kabul: 9.03.2021* *Araştırma Makalesi/Research Article*

Israeli-Palestinian Cyber Conflict

Mohammed Abu Saada[1]

Yıldırım Turan[2]

İsrail-Filistin Siber Çatışması	**Israeli-Palestinian Cyber Conflict**
Öz	**Abstract**
Filistin'in siber becerileri hala oluşum aşamasındadır. Öte yandan İsrail'in siber kapasitesi Filistin'in yeni gelişmekte olan becerileri ile kıyaslanamaz. Zira İsrail'in siber becerileri üst düzeyde ve uluslararası ölçektedir. Filistin-İsrail arasındaki siber mücadelenin en önemli araçları arasında siber korsanlık ve Facebook operasyonları yer almaktadır. Ancak siber mücadele alanında İsrail, Filistinlilere karşı açık ara öndedir. Bu da İsrail'in Filistin'deki telekomünikasyon ve internet altyapısına neredeyse tamamen hâkim olmasından kaynaklanmaktadır. Buna rağmen Filistinli siber gruplar, gerçekleştirdikleri siber korsanlık saldırılarıyla İsrailli politikacıları şaşkınlığa düşürmüştür. Bununla beraber Filistin-İsrail arasındaki siber saldırıların giderek tırmanan bir eğriye sahip olduğuna dair göstergeler bulunmaktadır.	Palestinian cyber capabilities are still at their early formative stage, On the other hand, Israeli cyber capabilities are not comparable to the nascent Palestinian cyber capabilities. However, hacking and social media, particularly Facebook, are among the most important tools of Palestinian-Israeli cyber conflict, where Israel is much superior to Palestinians, mainly due to its control over the telecommunications and internet infrastructure in Palestine. Nevertheless, Palestinian cyber teams have confused Israeli politicians after succeeding to carry out effective hacking attacks against Israel. Evidently, there are signs that cyber-attacks between Palestinians and Israelis are likely to increase steadily.
Anahtar Kelimeler: Siber Savaş, Siber Saldırı, Hacklemek, Filistin-İsrail Mücadelesi, Dijital Demir Kubbe	**Keywords:** Cyberwars, Cyber-Attacks, Hacking, Palestinian-Israeli Conflict, Digital Iron Dome
JEL Kodları: H56	**JEL Codes:** H56

Araştırma ve Yayın Etiği Beyanı	Bu çalışma bilimsel araştırma ve yayın etiği kurallarına uygun olarak hazırlanmıştır.
Yazarların Makaleye Olan Katkıları	Yazar 1'in makaleye katkısı %50, Yazar 2'nin makaleye katkısı %50'dir.
Çıkar Beyanı	Yazarlar açısından ya da üçüncü taraflar açısından çalışmadan kaynaklı çıkar çatışması bulunmamaktadır.

[1] PhD Candidate, Sakarya University, Middle East Institute, mohammed.abusaada@ogr.sakarya.edu.tr
[2] Asst. Prof, Sakarya University, Middle East Institute, yildirimturan@sakarya.edu.tr

1. Introduction

Cyberspace has become a significant battleground and an integral part of current and future conflicts. In recent years, there has been an increase in cyber-attacks on political targets, vital infrastructure, and websites of trade companies. Cyber-attacks have been increasingly drawing international attention, given the fact that electronic attacks are no longer limited to state capabilities only, but even groups and organizations can also engage in them. Since 2012, the online operation for global jihadi groups has been observed to recruit activists, raise funds, disseminate propaganda, incite hate and aggression, collect information, and wage psychological warfare, before targeting the critical infrastructure of the adversary, using cyber warfare techniques. (Azani, 2014: 5). This made some countries see cyber-attacks coming from factions and groups as a threat to their national security (Tor, 2015: 92). The development of cyber conflict is largely due to the global nature of the Internet amid a lack of regulations. Therefore, cyberspace has become a battlefield, not so much different from traditional battlefields (Abu Mualla, 2017: 61), especially that the cyber security threats are borderless, as the cyber state has no borders, unlike the case in a classical war (Adamsky, 2017: 122).

Israel, which used to be wary of a broadly consistent and synchronized conventional attack by its neighboring Arab states, later became afraid of suicide bombing and missile attacks launched by Palestinian organizations (Tor, 2015: 93), but it has recently been facing incendiary kites and balloons along the Gaza border, in addition to Palestinian cyber-attacks (Shahaf, 2018). Although the Palestinian territory and its population has been subject to strict control by Israeli security services since 1967 (Amad Media, 2019), however, cyber-attacks, along with real conflicts on the ground, have become common to some extent (Israel-Palestine conflict spills into cyberspace, 2009), especially since the scope of the Palestinian cyber threat is taking on psychological warfare after targeting sensitive Israeli websites, besides causing economic damage, by targeting industrial control systems (Tor, 2015: 97). Therefore, this study aims to identify the Palestinian cyber capabilities that have enabled Palestinians to carry out cyber-attacks on advanced Israeli sites – through tracking the most important historical stations of the provision of the Internet and telecommunications in the Palestinian territories, addressing the factors that boosted Palestinians' interest in the Internet in general, and explaining the nature of perpetrators of cyber-attacks, whether they are amateurs or members of organized Palestinian factions. The paper also highlights the Israeli cyber capabilities, although it completely believes that the capabilities of Palestinians and Israelis in the cyber domain are incomparable, due to the superiority of the Israeli cyber capabilities.

The study will also address the most significant tools of Israeli-Palestinian cyber conflict, especially hacking and social media, specifically Facebook, being the most widespread social media over the world, to explore the implications of these attacks and on both sides.

The study is divided into three axes, the first addresses cyber reality in Palestine; the second is about cyber reality in Israel; and the third deals with the tools of the Palestinian-Israeli cyber conflict.

2. The Cyber Reality in Palestine

The period following the inception of the Palestinian Authority (PA) in 1994 witnessed important developments in the field of communications and information technology, where

the first official Palestinian effort was the establishment of a competent ministry for post and telecommunications in 1995, which was later renamed as the Ministry of Communications and Information Technology. The PA also signed an agreement to operate home phones with the Palestinian Telecommunications Company, established in 1995, which started its work as the first Palestinian telecommunications company in 1997 as an operator and provider of terrestrial communication services. In the same context, the Palestinian Information Technology Association of Companies (PITA) was established in early 1999, for companies officially registered in the field of information systems, where the union represents more than 90 companies in Palestine specialized in various fields of technology and information. The Palestine Information and Communications Technology Incubator (PICTI) was established in 2004 as a competent authority to provide consulting services in the field of information technology and software (Palestinian Central Bureau of Statistics 2010, 2010: 25).

The use of the Internet began in Palestine in 1999 intending to enable Palestinian society to communicate with all countries of the world (Aouragh, 2003: 43). In 1999, the first Palestinian website, the Birzeit University Website, was established (Skare, 2018: 61). One of the reasons the Palestinians are interested in the Internet is its ability to provide an electronic space capable of crossing borders, especially after Israel started building the separation wall in the West Bank in 2002 (Saleh, 2015: 590) and has imposed a blockade on the Gaza Strip since 2006 (Abu Shamala, 2017). In addition, the high unemployment rates in Palestine also contributed to Palestinian interest in the internet (Salah, 2014), where the unemployment rate in 2018 among Palestinians over 15 reached 30.8% in all Palestinian regions (Palestinian Information Center Wafa, 2020). In the Gaza Strip, "the most vital in the software struggle" (Skare, 2018: 75), the unemployment rate was 52% (Palestinian Information Center Wafa, 2020). It is to be mentioned that the Palestinian people is considered one of the most educated people in the Middle East region, where in 2015, the educated people in Palestine reached 96.7%, which places the Palestinians at the forefront of Arab countries (Saleh, The Palestinian Strategic Report 2014-2015, 2016: 367). Also, the number of subscriptions to mobile cellular communications in Palestine increased by the end of 2019 to reach 4.2 million subscriptions, compared to 2.6 million subscriptions in late 2010, an increase of 63%. Also, the total number of ADSL high-speed internet subscribers in Palestine increased to about 363 thousand subscribers in late 2019, compared to about 119 thousand subscribers at the end of 2010, an increase of 205%. The results of a household survey for information and communications technology for 2019 show that 80% of Palestinian families have got an internet provider with 84% in the West Bank and 73% in the Gaza Strip (The Palestinian Central Bureau of Statistics, 2020).

However, the development of cyber infrastructure in the Palestinian territories has remained slow. This is due to the reliance of the Palestinian telecommunications companies, such as the "Mobile" company, established in 2000 (Palestinian Central Bureau of Statistics 2010, 2010: 25), on the Israeli telecommunications infrastructure, most of which follows Bezeq, an Israeli telecommunications company, according to the 1993 Oslo Accords. Accordingly, calls are transferred from anyone in the Palestinian territories to any other person in any local or international area through the Israeli infrastructure, which gives Israel control over any Palestinian digital activity. The Israeli Bezeq company justifies this by alleging that it considers it illegal for Palestinians to use electronic communications as tools against them (Skare, 2018: 62). It is to be mentioned that the establishment of the "Mobile" company

came later than other regional countries. In Jordan, for example, the first license to operate a public mobile phone service was granted to the Jordan Mobile Phones Company (Fastlink) in 1994, that is, six years before the Palestinian "Mobile" company (Palestinian Central Bureau of Statistics 2010, 2010: 28).

Despite this, the first Palestinian cyber activity emerged in 2000, when Palestinian hacker groups were established in the wake of the Israeli cyber-attacks against a website affiliated with the Lebanese Hezbollah (Allen & Chris C, 2003). Palestinian interest in cyber science increased in January 2012 when Israel came under electronic attacks, carried out by an Arab hacker called "Ox Omer" from Saudi Arabia, linked to the "XP" group (Middle East Online, 2012), where he targeted the Tel Aviv Stock Exchange and El Al Airlines websites. Ox Omer called on all Muslim hackers to join his online fight against Israel, which opened the eyes of the Palestinian parties to the importance of the software struggle. Accordingly, Hamas called for electronic jihad, where Hamas Spokesman Sami Abu Zuhri said that the "Ox Omer attack opened a new arena for Palestinian resistance against Israeli crimes (Skare, 2018: 12)." This encouraged Palestinian youth to enter the virtual world of "social media" in response to the Israeli's heavy use of it (Abu Mualla, 2017: 533), especially that more than a million Palestinians (mostly young) have Facebook accounts (Abu Mualla, 2017: 54).

Although most of the electronic devices owned by the Palestinians are not sophisticated and that they have not been able to keep up with the Israelis that always have the latest technology, in addition to the fact that the network connection in Palestine is not fast enough, according to the international speed standards, however, estimates indicate that there are more than 2500 professional Palestinians, most of whom are from the Gaza Strip (Qutb, 2016). Also, Palestinian cyber teams have emerged in Palestine, where almost all of them are located in the Gaza Strip, with only a team formed in the West Bank, called "The Wrath of Palestine", whose members later withdrew to maintain their social life (Skare, 2018: 144). Following are the key cyber teams in Palestine that can be divided into two parts, as follows:

First: Organized Palestinian Cyber Teams (professional)

The professional Palestinian cyber teams are the teams belonging to the armed Palestinian resistance factions, specifically Hamas and Islamic Jihad, as Islamic parties have come to believe that electronic resistance is very useful. Therefore, the electronic units of the Hamas and Islamic Jihad movements can be considered as arms that complement the work of their armed brigades (Skare, 2018: 190).

The key cyber teams that are influential in the Palestinian-Israeli conflict include:

1- The cyber division affiliated to the Palestinian Hamas movement:

The founder of the Hamas movement, Sheikh Ahmed Yassin, had stated that his movement would follow all available means to confront Israel, including the Internet. Experts describe the conflict between Hamas cyber units and Israel as amounting to a cyber war (Skare, 2018: 133). It is to be mentioned that Israel assassinated one of the leaders of the military wing of Hamas (Hamza Abu Al-Haija) after his location was determined through his personal account on Facebook (Abu Amer, 2015). In 2017, reports revealed that Palestinian women participated in cyber training during a recruitment campaign for Hamas (Dostri, 2018). The entry of Hamas into the field of "cyber war" came as a new method to be added to the movement's pursuit of attacking Israel and inflicting the greatest harm on it, whether by

sending messages to the Israeli community or obtaining sensitive confidential information that can be used to threaten Israel's security (Yassin, 2019). Therefore, Hamas is interested in strengthening its capabilities in the cyber domain, on the basis that cyber conflicts are likely to give Hamas intelligence victories, without incurring any significant cost. Although Hamas' current cyber capabilities do not pose a major threat to Israel, however, this can change relatively quickly, due to the rapid pace of its technological progress (Dostri, 2018).

2- The cyber teams affiliated with the Palestinian Islamic Jihad movement:

The Islamic Jihad movement started its electronic work in 1999 after a political decision (Skare, 2018: 141) that allowed this activity. The movement has an electronic unit within its armed wing, Al-Quds Brigades, called "Al-Quds Brigade" which was founded in 2008 (Skare, 2018: 136). The goals of electronic warfare to the Islamic Jihad movement can be summarized in three main points:

a- To face and prevent Israel's cyber-attacks,

b- To prevent Israeli espionage and bugging, and

c- To spread the Palestinian cause in the world and the international media (Skare, 2018: 137).

However, the cyber activity of the Islamic Jihad movement was not limited to these defensive measures. Rather, it has overtaken them to more offensive operations against Israeli cyber infrastructure (Abdel-Fattah, 2009: 218).

The development of the capabilities of both Hamas and Islamic Jihad can be explained by a statement by the Islamic Jihad movement on external support it had obtained in the field of cyber (Skare, 2018: 141). Also, Hamas did not deny obtaining foreign support to develop cyber warriors in the Izz al-Din al-Qassam Brigades (Skare, 2018: 140). Anyway, there are reports circulated on Iranian support provided for the Palestinian movements Hamas and Islamic Jihad (Abu Amer, Iranian Influence in the Gaza Strip: Evidence and Implications, 2011: 2) in this regard. But the surprising thing here is the existence of Qatari cyber support for the Palestinian resistance movements, amid reports about Qatari investments worth millions of dollars in the Gaza Strip. However, the Qatari cyber support to Gaza can be explained as not being necessarily intended to increase Palestinian cyber capabilities against Israel. Rather, it is an attempt to test its electronic programs in the Gaza Strip, based on the economic base for the purchase of weapons that they must be tested before purchasing them. Being hostile to Saudi Arabia, Qatar is mostly preparing for a cyber war with Saudi Arabia (Skare, 2018: 143). It is to be mentioned that Aviad Dadon, who works in the Israeli Ministry of Security, stated that Qatar has provided Hamas in Gaza with a sophisticated technical and computerized system through which it manages war against Israel, where missiles are fired by remote control, enabling Hamas to manage war from a sophisticated technical operations room, adding that this explains the few deaths among Hamas fighters in the recent battles. It manages the war with advanced technological means without the need to appear and run the risk of Israeli bombing (Arab 48 website, 2014).

Second: Voluntary Palestinian Cyber Teams (amateurs)

Key voluntary Palestinian cyber teams include:

1- The Gaza Hacker Team:

The Gaza Hacker Team is one of the most famous Palestinian electronic struggle teams, which has been active since 2012 and has political goals (Paganini, 2017). The team consists of:

A- Leadership: It consists of three people: Mr. Leon, Kasper, and Claw, all of whom are Palestinians residing in the Gaza Strip.

B- The team: It consists of Palestinians in addition to some Arab volunteers.

C- The groups: They are divided according to specialization. There are groups to hack sites and others to hack devices and emails.

What distinguishes the Gaza Hacker Team is that they do not know each other, so they only communicate through the Internet; thus, if any of them is exposed to danger, he does not endanger the rest (Skare, 2018: 84). The Gaza Hacker Team also denies affiliation to any Palestinian faction. They define themselves as young people from Gaza. They do not receive any support from any faction, group, or political movement (Skare, 2018: 85). Their goal is to hack Israeli websites, to cause economic damage to Israel, causing Israelis to lose millions of dollars annually due to hacking and destruction of sites (Skare, 2018: 91), in addition to disseminating information about the current events in the Palestinian territories (Skare, 2018: 98). However, Gaza Hacker Team is not experts in hacking, because they rely on technological tools developed by others. However, this does not mean that the team does not constitute a threat to the Israeli cyber infrastructure (Skare, 2018: 101).

2- The KDMS Hackers Team:

The KDMS Hackers Team was leading the global news in 2013; while the KDMS hackers team focuses its attacks on Israeli cyber infrastructure (Skare, 2018: 173), however, it launched hacking attacks against WhatsApp, Facebook, and Alexa, which belongs to Amazon and provides traffic data on the commercial internet, and others (The Guardian, 2013). All this activity happened between 8-12 October 2013 (Skare, 2018: 173). However, the group did not last long, it officially ended in April 2014 (Skare, 2018: 174).

3- Other Palestinian teams:

There are other Palestinian teams such as the 'Al-Aqsa Martyrs Brigades', the armed wing of the Fatah movement - the Gaza Strip branch - that tries to hack Israeli websites, collect information, and weaken the morale of Israelis (Skare, 2018: 164).' Unit 67' affiliated to the Martyr Abu Ali Mustafa Brigades, the military wing of the Popular Front for the Liberation of Palestine (Arab 45 website, 2017), in addition to many other Palestinian hacking groups such as 'Hagar Gaza 2007' and 'Gaza Security 2008' (Skare, 2018: 74).

All in all, the Palestinian cyber capabilities are still in the process of formation, where the haphazard nature still dominates the formation of Palestinian cyber teams, despite the great desire and motivation of some Palestinian parties to enhance their cyber capabilities.

3. Israeli Cyber Reality

Israel is one of the countries that deal openly with technology societies (Zaytouna Translations Series 82, 2019: 18). In 1999, 13% of the population of Israel used the Internet, which was a leap compared to its neighboring countries in the Middle East, where Internet

users represented 1% of the population in the same year (Skare, 2018: 61). One of the factors behind the rise of the cyber sector in Israel was signing the Oslo Accords in 1993 (Skare, 2018: 55), which contributed to enhancing economic security in Israel and encouraged the company's engagement in working in the electronics sector. Note that major companies had been reluctant to work inside Israel before Israel and Palestinians signed the Oslo Accords, where foreign financial investment has flowed to Israel since then. While the volume of foreign investment in 1990 was 100 million, it multiplied 20 times in the following eight years. The massive immigration of Jews from the former Soviet republics between 1990 and 2000 also helped Israel engage heavily in the high-tech industry. A third of the immigrants who arrived in Israel at the time had experience in the scientific, technical, or professional sectors (Skare, 2018: 56). In addition, 46% of Israeli adults have completed their education in technical sciences, engineering, and mathematics (Zaytouna Translations Series 82, 2019: 6).

Therefore, Israel has presented itself to the world as a source of e-learning to several countries, which led the United States, a pioneer in the cyber domain, to express admiration of the development of Israel in cyber technology (Adamsky, 2017: 113). Consequently, the development of Israeli cyberspace has become an important input for the development of its international relations. Although Israel was only evaluated according to its military capabilities, it is currently assessed in terms of its cyber policy. In order to benefit from the position of Israel in the cyber field, there are more than 30 multinational companies that deal with Israeli cyber companies. In 2015, Israeli companies operating in the field of cyber invested $250 million, while their exports amounted to 3.5 to 4 billion dollars, representing more than 7% of the world's exports in cybersecurity (Adamsky, 2017: 119). In 2018, Israeli exports in electronic products and information security industry were estimated at about $5 billion (Eitani, 2019: 22). There were significant implications for Israeli cyber innovation at the international level, where Tel Aviv has benefited from it politically and diplomatically worldwide. Various countries have rushed to benefit from Israeli experiences in cybersecurity, such as Brazil, Russia, India, China, and South Africa, in addition to many Arab and African countries close to Israel, which indicates an increase in the normalization of Arab-Israeli relations (Adamsky, 2017: 124). Israel is also considered one of the advanced countries in the field of digital diplomacy, as it ranked eighth globally in the digital diplomacy report for 2016, surpassing developed countries such as Switzerland, Germany, Japan, Canada, Austria, Spain, and Sweden. Since 2015, the Israeli Ministry of Foreign Affairs has hired more than 75 employees, volunteers, and 8 experts in the Department of Public Diplomacy, added to 30 employees in the same department, where they are deployed around the world in diplomatic representation offices. The Israeli Ministry of Foreign Affairs oversees more than 350 digital and social channels on the Internet and about twenty websites in Arabic, Hebrew, English, Persian, and Russian through the Digital Diplomatic Division, in addition to more than 80 sites belonging to diplomatic representation offices around the world (Abdel-Aal, 2018: 17).

Despite the establishment of the MAMRAM Unit, the central computing system unit that provides data processing services for all arms and the general staff of the IDF, on 15 July 1959, under the command of Mordechai Kikion, primarily responsible for operating systems in the IDF's military and chaired by Colonel Noam Rosenfeld since March 2010 (Al Majd security website, 2020), however, the real beginning of Israeli cybersecurity began with the directives of the Israeli Ministry of Defense in 1997 of establishing the Tehila Unit, which was charged with coordinating the country's infrastructure in the age of the Internet, to provide security

for state institutions. By the end of 2002, the Israeli government has seen cybersecurity not only as a technical means to secure its institutions but as a huge political issue, which created a state of leadership awareness of the importance of information technology. This awareness of Israeli politicians came after two important events in Israel: the first was the assassination of Prime Minister Yitzhak Rabin in 1995, and the second was the events of 11 September (Adamsky, 2017: 114). The assassination of Prime Minister Rabin was a great shock to the Israeli intelligence service, not less than the shock of the 1973 war, which led the Israeli intelligence to think outside the box, a trend that was enhanced by Israelis after the September 11 incident, pushing Israel to strongly believe that it is necessary to absorb cyber threats. Accordingly, the Israeli government mandated the "Israeli Security Council" to outline the emerging risk strategies, where it recommended in a special resolution No. B-84 of 2002 to protect computerized systems in the State of Israel and protect the central and sensitive infrastructure of the state. The Security Council also defined the goals and means of Israeli cyber security (Adamsky, 2017: 115).

Following these recommendations, the Israeli National Computer Bureau (INCB), affiliated with the Prime Minister's Office, was established. In 2011, according to the Israeli government resolution No. 3611, the International Narcotics Control Board was tasked with promoting the national cyber policy. The Israeli decisions aimed to enable Israel to achieve comprehensive defense while preserving its position as a global cyber power (Adamsky, 2017: 116). Israeli Prime Minister Benjamin Netanyahu stated during the government meeting on 14 December 2012 that the electronic infrastructure in Israel was being subjected to cyber-attacks (Arab 48 website, 2012), adding that in light of this, "a year ago, the National Cyber Authority was established, to address these attempts by developing what he called a "digital iron dome", the main goal of which was to defend Israel from computerized terrorism. In 2015, the Israeli government issued resolutions 3443 and 2444 that stipulated a national cyber security regulation mechanism for security needs (Adamsky, 2017: 116). Note that there have been other reasons for Israeli interest in cyber for military and security purposes, most prominently Israel's desire to achieve what may be called a cumulative deterrent, that is to convince its enemies that they have no way with Israel (Tor, 2015: 103), especially after General Uzi Moskowitz, head of the IDF communications and information technology unit, revealed that Israel would not be prompted to fight conventional wars in the coming years, but may fight wars that rely more on information and communications technology, with a large role for the cyber warfare (Arab 48 website, 2016). Throughout the twentieth century, Israel was wary of a broadly consistent and synchronized conventional war from its neighboring Arab states or being exposed to Palestinian suicide attacks. However, Israel has succeeded in achieving a kind of deterrence concerning attacks and conventional war by possessing a nuclear weapon, and through repeated military attacks against enemy targets (Tor, 2015: 102).

The Israeli IDF also plays a major role in leading the Israeli youth into the technology field through elite (Unit 8200) previously known as (Unit 848) with about 5,000 personnel (Security alliance, 2018), reporting to the Israeli Military Intelligence Service (AMAN) (Eitani, 2019: 15). The unit is responsible for collecting signal intelligence (SIGINT) and code decryption. Some sources indicate that the unit was established before 1948, from a group of young people who tried to develop their technological skills by collection and decryption of data about British and Arab opponents, and in 1950, the unit obtained a budget of $15,000 (Eitani, 2019:

12)The unit manages one of the largest intelligence signals bases in the world in the Negev known by Israelis as Urim, through intercepting phone calls and e-mail messages throughout the Middle East, Europe, Asia, and Africa, as well as tracking ships. According to some researchers, this unit is one of the best military intelligence agencies in the world, and some see it as paralleling the US National Security Agency (Eitani, 2019: 16). Note that Unit 8200 has established many leading companies worldwide, including Check Point Software Technologies Ltd. in 1993, Palo Alto Networks in 2005, and others (Eitani, 2019: 19). Unit 8200 is concerned with many tasks, including collecting data about Palestinian sexual orientation, betrayals, financial problems, family and medical conditions, and other privacy issues, to use them as pressure cards on Palestinians to become cooperative Israeli authorities or to create divisions in the Palestinian community. (Eitani, 2019: 30). Unit 8200 also collects communications data from Europe, the Middle East, and Africa, using a range of satellite dishes spread throughout Israel (Security alliance, 2018).

In addition to Unit 8200, there is Unit 3060, a secret intelligence unit reporting to the Military Intelligence Service "AMAN", which was established immediately after the end of the Israeli war on Gaza in 2014. Note that she was specialized in developing special security applications for computers and mobile phones of senior IDF officers, to protect them from penetration or steal information when lost. This unit has recently been unveiled, specifically in January 2020 (Al-Majd security website, 2020).

Also, there is Unit 9900, a special unit specialized in everything related to geography, including mapping and interpretation of aerial and satellite imagery and space research (IDF website, 2014), the Electronic Warfare Unit, the Military Computer Corps, the Signal Corps, and other electronics-dependent units of varying degrees, noting that the IDF supervises the training of Israeli youth on the use of advanced technology. The researches related to "wireless communications" and "data security networks", especially encryption, have come at the forefront of Israeli military researches (Skare, 2018: 58).

Despite the great Israeli cyber capabilities, there are several weaknesses in Israeli cyber security. Many former leaders of the Israeli security services have warned against an emerging phenomenon that they considered to be very dangerous, whereby former soldiers and officers sell their vast experience in the field of electronic hacking and counter-hacking to various countries all over the world. This warning came after several intelligence agencies in the world succeeded in employing many Israeli youths who had worked in the IDF cyber-attack units, such as Unit 8200, against attractive financial salaries that start from $20,000 up to $100,000 a month. Interestingly, this activity is no longer limited to only former army personnel but extended to several Israeli businessmen, some of whom had had senior positions in Israeli intelligence services, who have established foreign companies outside Israel, specializing in "cyber" and recruiting young men who had been demobilized from Israeli cyber units, and sometimes recruiting a person and all those who used to be under his command in the army (Asharq Al-Awsat website, 2019). Among the Arab countries that employ some Israeli cyber experts in the United Arab Emirates, specifically the Dark Matter company, established by Faisal Al-Bannai in 2014, and considered the commercial arm of the Cyber Division of the Emirates Intelligence and identifies itself as "a defense and digital intelligence company". The UAE has also succeeded in hiring several Israelis who had worked for the Israeli NSO Company, which has become well-known worldwide following its development of "Pegasus" software that controls mobile phones for espionage purposes. The

cost of Pegasus software is estimated at tens of millions of dollars, after which the party that uses it pays for NSO other amounts after each time he uses it. Estimates indicate that the UAE has paid nearly $100 million (Arab 48 website, 2019) to the Israeli company. One of the most important factors that lead to leakage of Israeli cyber information is a failure of the IDF to implement laws that protect copyright and intellectual property in cyber information to transfer knowledge directly to the expertise of ex-Israeli officers and soldiers in the technology sector when they finish their service (Skare, 2018: 58).

4. Tools of Palestinian-Israeli Cyber Conflict

There is an evolution in the tools of the Palestinian-Israeli cyber conflict. Although the early uses of the Palestinian cyber were through awareness campaigns and civil-political disobedience, sit-ins, and demonstrations, yet they developed to launching armed attacks targeting Israelis (Skare, 2018: 22). Recently, the most important and common tools of the Palestinian-Israeli cyber conflict include:

First: electronic hacking

Mostly the Palestinian-Israeli hacking struggle started in the late 1990s, but it increased significantly with the outbreak of the second Palestinian intifada (uprising) in September 2000. In late January 2001, the conflict-hit more than 160 Israeli websites and 35 Palestinian websites (Allen & Chris C, 2003). From 1999 to mid-April 2002, 548 Israeli websites were hacked. Gilad Rabinovich, the CEO of Netvision, the Israeli Internet service, says that what we were exposed to is considered an Internet uprising, but we started it when we put our flag on the Hezbollah website, and we woke them up. Following are the most important hacking operations that took place between the Israeli and Palestinian parties:

1- Israeli hacking operations:

In late December 2008, the Israel Defense Forces (IDF) hacked a Hamas TV channel and broadcast a series of cartoons depicting the death of the Hamas leadership under the title “Time is running out” (Leyden, 2009).

During the war on Gaza that lasted for July and August 2014 (Abdel-Hamid, 2014: 7), a group of programmers working under the name of “Help Israel Win” has disabled four different Hamas’s news websites (The Guardian, 2013).

On May 5, 2019, Israeli warplanes launched an airstrike on a building housing Hamas Internet activist (Borghard & Schneider, 2019). The commander of the Israel Defense Forces cyber division explained that the Israeli airstrike came after Hamas carried out a cyber-attack on Saturday 4 May 2019, which was designed to “harm the quality of life of Israeli citizens”. The cyber operation targeting the Hamas movement was a collaborative effort between the elite Unit 8200 of Military Intelligence, the IDF’s Teleprocessing Directorate, and the Shin Bet security service. It is believed that this is the first time that the military has retaliated with physical violence in real-time against a cyberattack.

Although the US used drones to kill Junaid Hussain, the ISIS senior hacker in August 2015, the American cyber/military response was targeting an individual, while Israel targeted an entire building (Cropsey, 2019).

2- Palestinian hacking operations:

In the early beginnings, the Palestinian software struggle was aimed at hacking Israeli websites to transfer the image of Palestinian suffering to an audience that the Palestinian cannot reach in real life (Skare, 2018: 65).

The most important Palestinian hacking operations against Israeli websites included:

In 2002, Palestinian Authority security officers hacked Israeli reconnaissance drones flying above Gaza and the intercepted footage was relayed to Hamas (Zilber, 2020).

In 2008, the Palestinian hackers carried out many cyberattacks against Israeli sites (Skare, 2018: 83), most of which coincided with the Israeli war on Gaza in late 2008 (Hoteit, 2009: 213). One of the most important successful attacks was carried out by the Gaza hackers' team, which in February 2009 targeted the Israeli Kadima party led by Israeli Prime Minister Ehud Olmert (carr, 2010: 25).

On October 23, 2012, the Israeli police found out that all their computers were hacked and that it took them a week to find out this. The Israeli government accused hackers of Gaza of being behind the hacking (Skare, 2018: 82). During the Israeli military offensive on Gaza, Operation Cast Lead, in 2012, Hamas assumed responsibility for cyber-attacks on Israeli websites, including the Home Front Command website and the IDF Spokesman website (Dostri, 2018).

In February 2013, Israel accused the Hackers Team of a cyber-attack that led to the closure of the Haifa tunnel for two days. The estimated costs of the attack amounted to hundreds of thousands of dollars (Skare, 2018: 93). However, the largest hacking operation in 2013 came on April 7, 2013, after a group of "hackers" managed to penetrate and destroy sensitive Israeli pages and websites, including the Israeli Ministry of Defense website and the Mossad website, in addition to the websites of both the Prime Minister and the Ministry of Trade and Industry, the Israeli Stock Exchange, and the Israeli Ministry of Justice's Court Affairs, the Haifa Police, the Tel Aviv Police, and some news websites, in addition to banks, tens of thousands of Israeli accounts on the social networking sites, estimated at 40,000 pages and accounts. Accordingly, classified documents were published on the Internet containing names of agents recruited for the Mossad, including Arabs, and data on Zionist officers and settlers on the Internet, in addition to credit card data and bank accounts, and the data of the Ministry of Trade and Industry (Khalifa, 2017).

In February 2014, Israel accused the Gaza Hackers of attacking the Civil Administration in Judea and Samaria, the Israeli government agency that deals with all administrative matters in the West Bank (Skare, 2018: 83). In February 2014, Hamas also succeeded in penetrating Israeli army monitoring systems in the West Bank. The aim was to prevent the Israeli army from collecting information via surveillance cameras deployed throughout the West Bank and to impede the army's ability to use its monitoring system to thwart Palestinian operations against Israeli targets. The Hamas electronic attack also aimed to monitor the movements of Israeli soldiers in West Bank cities and regions to carry out attacks against them (Yassin, 2019). With the flare-up of the Israeli war on Gaza in 2014, Palestinian cyber-attacks increased 500% after Palestinian hackers succeeded in targeting the websites of Israeli civilian government agencies, financial services, and military agencies - including the Mossad (Frizell, 2014) Israeli intelligence service. Among the Palestinian cyberattacks, Hamas transmitted TV broadcasts via a ground antenna to the homes of Arab Bedouins in southern Israel during the

war on Gaza (Zilber, 2020). In addition, the Al-Qassam Brigades succeeded to hack Israeli TV channels, including the tenth and second channels, during the war, and broadcast warning messages to Israeli society (Yassin, 2019).

In January 2017, dozens of phones belonging to Israeli soldiers and officers were hacked by Hamas (Dostri, 2018). The aim was to eavesdrop on their calls and messages and hack their data. In October 2017, Palestinian elements succeeded in penetrating the army's radio signal frequencies and spying on a conversation between members of a military force stationed on the border with Gaza (Yassin, 2019). During the same year, the Martyr Abu Ali Mustafa Brigades, the military wing of the Popular Front for the Liberation of Palestine, announced that Unit 67 of the electronic security team succeeded in hacking hundreds of Israeli phones, in solidarity with Palestinian prisoners in Israeli prisons (Arab 45 website, 2017).

In July 2018, the IDF revealed that Hamas launched a sophisticated cyberattack using fake files for women on social networks to control the soldiers' mobile phones and their computers. Hamas also attempted to attack soldiers through WhatsApp. Hamas was able to access the microphone and camera of mobile phones, without the knowledge of their owners. As part of this attack, Hamas opened a Facebook group related to the 2018 FIFA World Cup and invited soccer fans to join the group to get updates, watch live broadcasts, and wager on games. Users who joined the group and clicked on its links were exposed to internet breaches and hacking of their computers. Meanwhile, information security company "ClearSky" revealed in August 2018 that Hamas tried to plant spy programs on mobile phones belonging to Israelis, using an application that simulates the "Red Alert" application (Dostri, 2018).

On May 15, 2019, Palestinian hackers attacked an Israeli broadcast on the Internet for a 10-minute Eurovision semi-final, broadcasting scenes of fake explosions near the Eurovision site in the host city, Tel Aviv, together with animated video and siren sound, with a warning saying: "Israel is not safe. You will see." Israeli radio accused the Hamas movement of being behind the hacking operation (BBC News, 2019).

The above-mentioned Palestinian hacking operations come in the context of a model of Palestinian electronic attacks, but not limited to them, where estimates indicate that in 2012, Israel was exposed to more than 44 million electronic attacks (CNN Arabic, 2012). It is also worth noting that the high-quality successes achieved by the Palestinian electronic units in hacking several websites, including the success of security services in Gaza in revealing the identities of dozens of spies recruited by the Israeli intelligence, which was achieved when Palestinian hackers penetrated the servers of an Israeli security agency and recovered the list of Palestinian agents (Abu Amer, Hamas' cyber battalions take on Israel, 2015). Also, the electronic committees of the Palestinian factions succeeded more than once in landing Israeli drones that were flying over Gaza and seized the information and pictures that they were taking (Yassin, 2019).

The study explains that the number of Palestinian hacking attacks against Israel is greater than the Israeli attacks against the Palestinians. But this does not mean that the Palestinian cyber capabilities are better than the Israeli capabilities, or even close to them, but this is due to several other reasons, most prominently:

- Israel's heavy reliance on technology expands the cycle of risks that it may be exposed to, given the fact that Israel is one of the leading countries in the field of technology in

general; and its dependence on computers and artificial intelligence is increasing to manage many vital domestic sectors, such as electricity, water, factories, control and navigation systems, and others. Hence, the Palestinians see that this as being in their favor, where they can damage Israeli interests. On the other hand, Israel does not find a significant adoption of technology in the lives of Palestinians, which narrows the scope for Israeli hacking operations.

- Israel's regional and international competitive preoccupation: Perhaps Israel does not currently see that the Palestinian capabilities are large and require an electronic preoccupation with them, considering Israel's focus on maintaining its international position in the field of cyber production. Moreover, it focuses its cyber-attacks on those that Israel believes to be a threat to its national security, such as Iran, Turkey, and some Arab countries.

- Israeli hegemony over the Internet in Palestine: Through its foundational and training role in developing the telecommunications network in Palestine, Israel may be aware of the smallest details, which does not push it to more hacking attacks.

- The security nature of Israel does not allow it to disclose its security operations in general and cyber-attacks in particular. This means that Israel may carry out millions of hacking operations against the Palestinians without declaring them, in case it cannot impose semi-cyber censorship on everything electronic belonging to Palestinians.

Second: digital diplomacy "social media pages"

The study will shed light on Facebook, being the most famous social media all over the world, ranking first compared to other social media with about 2.45 billion users per month globally, while Twitter users are estimated at 330 million Snapchat users 360 million, and Instagram users up to one billion (Kellogg, 2020).

The Palestinian-Israeli conflict began to materialize when Facebook removed Palestine from the drop-down list containing names of countries that users choose when signing up for a new account, thus stripping Palestinians of their right to choose their place of residence, which sparked a heated debate that forced Facebook to restore Palestine to the list (Abu Mualla, 2017: 55). With Facebook entering the Palestinian-Israeli conflict, Israel created many pages, most notably:

Al-Munasek," the Arabic-language Facebook page of COGAT, Israel's liaison body for coordinating activities in the Palestinian territories.

- Al-Munasek (Coordinator) page: This Arabic-language Facebook page was launched in March 2016, identifying as: "the "Coordinator of Government Activities in the Territories" (COGAT), an Israeli liaison body for coordination of activities in the Palestinian territories. The promotion of the page came in coincidence with the accession of the State of Palestine to an observer member in the United Nations General Assembly in late 2012, and the change of its name from "Palestinian Authority" to Palestinian State. This page aims to undermine the concepts of the Palestinian State and Palestinian Authority in favor of the so-called "Coordinator" on Facebook that intends to create virtual relations with the Palestinians to turn into real relations on the ground by requesting provision of services, humanitarian assistance, and others, which aims to surpass the role of the State of Palestine and its institutions. The Coordinator Facebook page that has over half a million followers (Amad Media, 2019), was exposed in May 2020 to a Palestinian awareness campaign to urge Palestinians to unfollow and even boycott the "Coordinator" page, which led to the withdrawal of more than 100,000 followers from the page (Mousa, 2020).

- The Facebook page of Avichai Adraei, the Israeli occupation army spokesman in Arabic, aims to penetrate Palestinian and Arab public opinion and influence its beliefs. It is no longer strange that you see “Adraei” reading verses from the Qur'an in an attempt to prove that resisting Israel is wrong. Over a million people (Amad Media, 2019) follow the Avichai Adraei Facebook page (Abu Mualla, 2017: 56). Since Gaza is the most strained area and is usually the hottest battleground between Palestinians and Israelis, it is natural that Gaza has the largest number of visitors to this page. Israel has also created many Israeli pages in Arabic, including a page called “Israel speaks Arabic”, affiliated to the Israeli Ministry of Foreign Affairs (Abu Mualla, 2017: 55), which seeks to present Israel to the Arab community as a humanitarian country (Abu Mualla, 2017: 56), and a page called “Israel uncensored” that posts pictures of Israeli cities, as well as Israeli cultural and scientific news, with over one million followers, mostly from Cairo, especially those between 18-24 years old. There is also a Facebook page for Israeli Prime Minister Benjamin Netanyahu (Abu Mualla, 2017: 57).

There are reports that the functions of the Israeli Facebook pages go beyond the apparent intentions to maintain peaceful communication, as numerous reports have indicated that there is a relationship between Israeli social networking sites and Tel Aviv’s pursuit to recruit potential Palestinian collaborators, especially young men, who are often subject to reward and punishment (Abu Amer, Hamas' cyber battalions take on Israel, 2015). In addition, Israeli intelligence has sought to change perceptions and attitudes of some Palestinians towards Israel and issues of concern to Israelis. Note that Israel also assigned Israelis who are fluent in the Arabic language and formed the “Hatsaf Unit” in 2003, a military unit accused of monitoring Arab social media pages as well as the Arab media (Abu Mualla, 2017: 58); and a unit called “Unit 3060”, a field intelligence secret unit affiliated to the Military Intelligence Service “Aman", which was created in the wake of the 2014 Israeli war on Gaza. Unit 3060 collects pictures, reports, videos, ads, statements, social media posts, maps, and location of events, to be analyzed, made available, and provided to intelligence officers (Al-Majd security website, 2020).

Despite the great Israeli superiority in the conflict run via social media, however, there are successful attempts by Palestinian individuals who seek to refute Israeli propaganda and exposing Israeli violent practices, through addressing Western public opinion. Examples of these successful Palestinian models include:

- Eisa Amr from the city of Hebron, head of a youth association against settlements,

- Manal Al-Tamimi from the Nabi Saleh village, north of Ramallah, a member of the Popular Committee to Resist the Wall,

- Jana Al-Tamimi, an 11-year-old Palestinian girl, also from the Nabi Saleh village, where a report by the Israeli Ministry of Strategic Affairs indicated that she poses a strategic threat to Israel because she documents Israeli attacks on her village and disseminates them through her account on Twitter that has hundreds of thousands of followers. A graphic report or a video clip posted by Jana on Twitter usually receives more than 20 thousand views (Amad Media, 2019).

- Farah Baker, a Palestinian girl from Gaza City, who was described by the American magazine “Foreign Policy”, as “an international media sensation, attracting hundreds of thousands of Twitter followers”, one of the most influential people in the world in 2014 as she was “live-tweeting to document the war unfolding around her… the Israeli bombs and

rockets exploding outside her home in Gaza", highlighting and documenting Israeli crimes and posting them on Twitter in English.

- Ahmed Joudeh from Gaza, accompanied by a group of young people, launched a Palestinian campaign called "Ihbid" (Expose Lies), to expose the Israeli narrative wherever it is, and which was very popular on social media. The campaign pursues posts and tweets that promote the Israeli occupation narrative against Palestinians on social media, where young Palestinians send thousands of comments on these posts in different languages supported by links and pictures of the Israeli crimes committed against Palestinians. The campaign came spontaneously after these activists sent tens of thousands of intensive comments to the National Geographic Channel based in Abu Dhabi to delete a post speaking about a Palestinian desert in Hebron under its Israeli name instead of using its real Palestinian name "Ein Gedi Desert", which prompted the channel to republish new content with the correct Palestinian name, deleting the Israeli name. Among the accomplishments of the "Ihbid" campaign, Joudeh says that on the anniversary of the Nakba on May 15: "In three hours, our activity reached more than 21,000 tweets on Twitter about our adherence to the right of return. Moreover, the young people internationalized the campaign, as they included the hashtag #Ihbid194 in their comments, linking it with UN Resolution 194 related to the right of Palestinian refugees to return to their homes from which they were displaced in 1948, in addition to the fact that No. 194 is the number of the State of Palestine's membership in the United Nations (Prose, 2015).

Despite they are limited, the Palestinian successes in the Facebook arena are disturbing to Israel, which explains why Israel follows the policy of blocking Palestinian Facebook pages. Although Israel is more powerful in cyberspace, it asked the Facebook administration to block some Palestinian pages like the "Third Palestinian Intifada" page that had attracted about half a million users. The Facebook decision came after Israeli Minister of Public Diplomacy Yuli Edelstein sent a message to Facebook founder Mark Zuckerberg complaining that the Palestinian page blatantly calls for killing Jews and liberation of Jerusalem using violence. Also, some Facebook pages belonging to accounts for Hamas leaders have been closed, including Hussam Badran and Izzat Rashq. Palestinian news pages were also blocked, including the page of Watan News Agency, on the pretext of inciting hatred (Abu Mualla, 2017: 59).

However, the developed Israeli capabilities in cyberspace do not mean that it controls everything. On the contrary, Israeli reports indicate that the social networks owned by the Hamas movement were more effective than the Israeli pages during the Israeli attack on Gaza in 2014. Likewise, the individual initiatives of some Palestinian young people on Facebook have dealt with painful blows to Israeli cyberspace (Abu Mualla, 2017: 60). This explains why Israel arrested more than 150 Palestinians during the period between October 2015 to February 2016, based on posts and shares on Facebook, in which they expressed their views on the 2014 Gaza war (Skare, 2018: 63).

To sum up, when we compare Israeli digital diplomacy with Palestinian digital diplomacy, we find that the result is definitely in favor of Israel. This is due to the challenges posed by the almost complete Israeli electronic control, in addition to the fact that the Palestinian Authority is still in the process of building state institutions now. Moreover, the Palestinians do not have a specific strategy for digital diplomacy, as there is no department or section in the Palestinian Ministry of Foreign Affairs for activating digital diplomacy. This explains the

significant difference between the Palestinian Authority and Israel concerning the level of presence in the cyberspace, and accordingly the poor content provided by Palestinians in this regard on the Internet. While every Israeli ministry includes a section for digital diplomacy, and most politicians and ministers have their accounts in more than one language on several electronic platforms, some Palestinian officials do not even have effective accounts on the Internet, and some others use the social networking sites via their accounts, in the absence of a professional system with a specific strategy. Meanwhile, Israel allocates huge budgets for the promotion of tweets and posts on Twitter, Facebook, and other international media (Amad Media, 2019). The study suggests that despite the challenges that face the Palestinian cyber capabilities, a significant segment of Palestinians now believe that their cyber capabilities can play a key role in the Palestinian-Israeli conflict, which requires working hard to boost and develop their skills in this regard. Given that Israel relies heavily on technology, any potential Palestinian cyber-attacks can have extremely serious consequences for Tel Aviv, particularly on its commercial sector. In this regard, it is expected that some Palestinian parties may resort to external capabilities to get advanced training courses in cyber technology. In this context, it is also expected that some young Palestinians overseas may seek obtaining academic degrees as well as up-to-date courses in computer science in general, and in cyber technology in particular, in countries that offer free scholarships such as Turkey, Iran, Malaysia, India and others. In this case, Israel will most likely consider maintaining its assassination policy to target any Palestinian that acquires qualitative cyber capabilities that may pose a threat to Tel Aviv.

5. Conclusion

Considering the Palestinian cyber-attacks against Israel so far, particularly those undertaken by Hamas, they can be described as more daring to tactics. These attacks enabled Palestinian hackers to obtain sensitive information after their success in hacking some Israeli devices and websites. In addition to the success of the Palestinian hackers in breaking the siege imposed on them and delivering their messages through the electronic space, the Palestinians have benefited from their electronic cyber activity in promoting Palestinian identity through the use of pictures and slogans related to the Palestinian Revolution. However, the Palestinian technological capabilities have not developed so much to the extent that they could cause massive harm to Israel; and accordingly, it is doubtful that they would pose a real threat to Israel in the coming years. Nevertheless, the Palestinian cyber capabilities are evolving, which would affect the quality and quantity of direct electronic attacks against Israel, where these attacks are likely to increase and expand if Palestinians respond to challenges and requirements of engagement in the world of electronic warfare effectively, especially since Israel has not reached the stage of establishing total deterrence of its enemies in cyber technology. The Palestinian factions, especially those that are close to Iran, want to establish a communication network of their own so that they can avoid being subject to Israeli security control. In addition, they have limited efforts in the achievement of technological development in their military industries, drones, and missiles, to enable them to become more accurate. Thus, cyber conflicts remain of concern to Israel, even if they come from emerging organizations. The Israeli military doctrine is based on two principles, early warning, and decisive response, i.e. prior knowledge and devastating short war. However, this Israeli strategy has become ineffective with cyber conflicts due to the absence of decisive Israeli capabilities.

References

Abdel-Aal, W. (2018), *Palestinian Digital Diplomacy and Its Position in Palestinian Foreign Policy.* Birzeit: Media Development Center - Birzeit University.

Adamsky, D. (2017), The Israeli Odyssey toward its National Cyber Security Strategy. *The Washington Quarterly*, vol. 40, no. 2: 113–127.

Abdel-Fattah, N. (2009), *Electronic Terrorism, Power in International Relations, a New Pattern and Various Challenges.* Cairo: Center for Political and Strategic Studies.

Abdel-Hamid, M. (2014), *The aggression against the Gaza Strip, the Palestinian situation between internal and external rivalries.* Ramallah: Center for Democratic Republic Studies.

Abu Amer, A. (2011), *Iranian Influence in the Gaza Strip: Evidence and Implications.* Jerusalem: Friedrich Ebert.

Abu Amer, A. (2015), *Hamas' cyber battalions take on Israel*. Retrieved May 6, 2020, from Al-monitor.

Abu Mualla, S. (2017), Palestinian - Israeli Cyber Conflict: An Analytical Study of the Israeli Propaganda on Facebook Adraei's page as an example, *Journal of the Arab American University*, vol. 3, no. 2: 52-75.

Abu Shamala, J. (2017), *The Siege of Gaza: Reality, Dimensions and Repercussions*. Retrieved May 2, 2020, from Rouya Turkiyyah Magazine: https://bit.ly/3eoAQFt, (Accessed: 02.12.2020).

Al Majd security website. (2020), *MAMRAM, The Computing Unit in the Zionist Army*. Retrieved from Al Majd security website: https://almajd.ps/news4834/, (Accessed: 22.11.2020).

Allen, P., & Chris C, D. (2003), *The Palestinian-Israeli Cyberwar*. Retrieved Nov 5, 2020, from ACADEMIC JOURNAL ARTICLE Military Review.

Al-Majd security website. (2020), *Learn about the selected unit in the occupation army,*. Retrieved from Al-Majd security website: https://almajd.ps/news9199/, (Accessed: 12.11.2020).

Amad Media. (2019), *Digital diplomacy is the newest arena in the Palestinian-Israeli conflict*. Retrieved April 19, 2020, from https://www.amad.ps/ar/post/303435, (Accessed: 22.11.2020).

Aouragh, M. (2003), *Cyber Intifada and Palestinian Identity.* Tübingen: ISIM NEWSLETTER.

Arab 45 website. (2017), *Cyber Attacks Targeted Hundreds of Israeli Phones*. Retrieved April 11, 2020, from Arab 45 website: https://bit.ly/2WeE0p0, (Accessed: 02.11.2020).

Arab 48 website. (2012), *Netanyahu: Israel is subjected to daily cyber-attacks, and we are building a digital iron dome*. Retrieved March 11, 2020, from Arab 48 website: https://bit.ly/30dyynM, (Accessed: 02.11.2020).

Arab 48 website. (2014), *An Israeli expert: Qatar is a superpower in the field of cyber and provided Hamas with advanced technologies*. Retrieved April 11, 2020, from Arab 48 website: https://bit.ly/3fpp9Q8, (Accessed: 02.11.2020).

Arab 48 website. (2016), *Israel's Coming Clashes: Not a conventional war nor an existential threat*. Retrieved March 11, 2020, from Arab 48 website: https://bit.ly/2BXWdQZ, (Accessed: 02.11.2020).

Arab 48 website. (2019), *Israelis Develop Cyber Offensive Programs for the Emirates Intelligence*. Retrieved April 11, 2020, from Arab 48 website: https://bit.ly/3frbGaD, (Accessed: 02.11.2020).

Asharq Al-Awsat website. (2019), *Israeli cyber companies sell their expertise to the world*. Retrieved April 12, 2020, from Asharq Al-Awsat website: https://bit.ly/3eoXvS3, (Accessed: 02.11.2020).

Azani, E. (2014), *international institute for counter- terrorism newsletter.* Herzliya: Cyber-Terrorism Desk.

BBC News. (2019), *Hackers interrupt Israeli Eurovision webcast with faked explosions*. Retrieved April 21, 2020, from BBC News: https://www.bbc.com/news/technology-48280902, (Accessed: 02.11.2020).

Borghard, E., & Schneider, J. (2019), *Israel responded to a Hamas cyberattack with an airstrike. That's not such a big deal*. Retrieved April 20, 2020, from Washington Post: https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/, (Accessed: 02.11.2020).

Carr, J. (2010), *Incide Cyber Warfaer.* United States of America: O Reilly.

CNN Arabic. (2012), *44 Million Cyber-Attacks Targeting Israel*. Retrieved May 1, 2020, from CNN Arabic: http://archive.arabic.cnn.com/2012/scitech/11/20/anonymous.declare.cyberwar.on.israel/index.html, (Accessed: 02.11.2020).

Cropsey, S. (2019), *Hamas Cyber Attack and Israel's Armed Response*. Retrieved March 30, 2020, from Hudson Institute: https://www.hudson.org/research/15016-hamas-cyber-attack-and-israel-s-armed-response, (Accessed: 02.11.2020).

Dostri, O. (2018), *Hamas Cyber Activity against Israel*. Retrieved May 12, 2020, from The Gerusalem Institute for Strategy and secutity: https://jiss.org.il/en/dostri-hamas-cyber-activity-against-israel/, (Accessed: 02.11.2020).

Eitani, F. (2019), *The Israeli Unit 8200 and its Role in Serving Israeli Spy Technology.* Beirut: Al-Zaytouna Center for Studies and Consultations.

Frizell, S. (2014), *Off the Battlefield, Hackers Are Waging Cyberwar Against Israel and Palestine*. Retrieved April 27, 2020, from Time: https://time.com/3089473/israel-gaza-hackers/, (Accessed: 22.12.2020).

Hoteit, A. (2009), *Studies in the Israeli aggression on the Gaza Strip* (Vol. I), Beirut: Al-Zaytouna Center for Studies and Consultations.

IDF website. (2014), *Autism in the IDF: Meet the Soldiers of Intelligence Unit 9900*. Retrieved May 2, 2020, from IDF website: https://www.idf.il/en/minisites/our-soldiers/autism-in-the-idf-meet-the-soldiers-of-intelligence-unit-9900/, (Accessed: 02.12.2020).

Israel-Palestine conflict spills into cyberspace. (2009), Retrieved April 30, 2020, from The Guardian: https://www.theguardian.com/technology/2009/jan/15/israel-palestine-online-conflict, (Accessed: 02.11.2020).

Kellogg, K. (2020), *The 7 Biggest Social Media Sites in 2020*. Retrieved May 13, 2020, from Search Engine Journal: https://www.searchenginejournal.com/social-media/biggest-social-media-sites/#close, (Accessed: 02.11.2020).

Khalifa, A. (2017), *Cyber Battles, Israeli Horror Scenario*. Retrieved March 12, 2020, from Ida2at website: https://www.ida2at.com/battles-of-the-cyber-israeli-horror-scenario/, (Accessed: 02.11.2020).

Leyden, J. (2009), *Israel hacks Arab TV station Cyberspace becomes battleground in Gaza conflict*. Retrieved March 12, 2020, from The Register: https://www.theregister.com/2009/01/06/idf_al_aqsa_hack/, (Accessed: 02.11.2020).

Middle East Online. (2012), *Cyber war: 'Gaza hackers' deface Israel fire service website*. Retrieved May 7, 2020, from Middle East Online: https://middle-east-online.com/en/cyber-war-gaza-hackers-deface-israel-fire-service-website, (Accessed: 02.11.2020).

Mousa, K. (2020), *The Palestinians use the account to find out the status of barriers and information regarding their entry permits to Jerusalem and Israel*. Retrieved Jun 1, 2020, from The Independent Arabic website: https://bit.ly/3euiCCq, (Accessed: 02.11.2020).

Paganini, P. (2017), *Gaza Cybergang is back and is targeting Governments under DustySky campaign*. Retrieved May 13, 2020, from Security Affairs: https://securityaffairs.co/wordpress/55840/intelligence/gaza-cybergang-dustysky.html, (Accessed: 02.11.2020).

Palestinian Central Bureau of Statistics 2010. (2010), *a comparative report on access of families and individuals to information and communication technology in the Palestinian Territories 2000-2009.* Ramallah: Palestinian Central Bureau of Statistics.

Palestinian Information Center Wafa. (2020), *Unemployment in Palestine*. Retrieved from Palestinian Information Center Wafa.

Prose, F. (2015), *Writing From a War Zone Doesn't Make You Anne Frank, Foreign Policy*. Retrieved Jun 1, 2020, from Foreign Policy: https://foreignpolicy.com/2015/05/15/writing-from-a-war-zone-doesnt-make-you-anne-frank-girl-emulated-farah-baker-zlata-filipovic/, (Accessed: 02.11.2020).

Qutb, H. (2016), *Beyond the Curtain: The Palestine Private Army ..." Hacked "Tel Aviv"*. Retrieved May 1, 2020, from Sasa Post: https://www.sasapost.com/tel-aviv-hackers-gaza/, (Accessed: 02.11.2020).

Salah, H. (2014), *Israeli websites hacking, a second raging front*. Retrieved May 1, 2020, from Al-Monitor: https://bit.ly/3fqnWZ5, (Accessed: 02.11.2020).

Saleh, M. (2015), *The Palestinian National Authority - Studies in Experience and Performance 1994-2013* (Vol. 1), Beirut: Al-Zaytouna Center for Studies and Consultations.

Saleh, M. (2016), *The Palestinian Strategic Report 2014-2015.* Beirut: Al-Zaytouna Center for Studies and Consultations.

Security alliance. (2018), *Spies in the Middle East: Israeli Cyber Operations*. Retrieved May 17, 2020, from Security alliance: https://www.secalliance.com/blog/spies-in-the-middle-east/, (Accessed: 02.11.2020).

Shahaf, T. (2018), *Hamas preparing for cyber war*. Retrieved Feb 7, 2020, from Globes: https://en.globes.co.il/en/article-hamas-preparing-for-cyber-war-1001246720, (Accessed: 02.11.2020).

Skare, E. (2018), *Digital Jihad; Palestinian Resistance in the Digital Era", translated by Mansour Al-Omari.* (M. Al-Omari, Trans.) Baghdad: Mediterranean Publications.

The Guardian. (2013), *Net security firm Metasploit's DNS registrar hacked – by fax*. Retrieved March 3, 2020, from The Guardian: https://www.theguardian.com/technology/2013/oct/15/metasploit-kdms-dns-hacked-fax, (Accessed: 02.11.2020).

The Palestinian Central Bureau of Statistics. (2020), *A joint press release by the Palestinian Statistics and the Ministry of Communications and Information Technology*. Retrieved sep 5, 2020, from The Palestinian Central Bureau of Statistics: http://www.pcbs.gov.ps/postar.aspx?lang=ar&ItemID=3737#, (Accessed: 02.11.2020).

Tor, U. (2015), Cumulative Deterrence as a New Paradigm for Cyber Deterrence. *THE JOURNAL OF STRATEGIC STUDIES*, vol.40, no.1-2: 92-117. doi:https://doi.org/10.1080/01402390.2015.1115975, (Accessed: 02.11.2020).

Yassin, H. (2019), *Cyber Warfare is a New Palestinian Weapon terrorizing Israel*. Retrieved April 1, 2020, from Al-Jazeera website: https://bit.ly/307CMwX, (Accessed: 02.11.2020).

Zaytouna Translations Series 82. (2019), *Innovation and the Artificial Blocks Series in Israel.* Beirut: Zaytouna Center for Studies and Consultations.

Zilber, N. (2020), *Inside the Cyber Honey Traps of Hamas*. Retrieved May 5, 2020, from Daily Beast: https://www.thedailybeast.com/inside-the-cyber-honey-traps-of-hamas, (Accessed: 02.10.2020).