The Geopolitical Implications of the Iranian-Israeli Cyber War for The Netherlands

30-06-2025

Hasan Alkhatib

Abstract

The rapid developments in modern technology and the near-total reliance of most countries on this technology have reshaped economic, political, and social relations. This is due to the significant role this technology plays in facilitating movement and communication between countries, enhancing cooperation, accessing necessary information at the required speed, and raising the efficiency of international economic activity to unprecedented levels. The cyber space is the ground upon which technology lives and thrives. The cyber space is an exceptional world that deviates from the traditional rules of the human world in which we live, and it has its own rules. For example, by virtue of nature, strength is the opposite of weakness. The stronger a person becomes, the less their weaknesses decrease. This is similar to the animal and plant worlds. In the cyber world, the more advanced a country's cyber capabilities and the more sophisticated its digital government becomes, the more vulnerabilities it has.

This exposes modern technology to very serious repercussions if misused or transformed into a tool of political and military conflict between countries. This has been happening over the past two decades between several countries, particularly between Iran and Israel. The conflict between these two Middle Eastern countries is escalating, and each is developing its own cyber tools and using them in its conflict against the other. Because cyber conflict takes place in a non-geographical space, the effects of a cyber conflict, or cyber war, between two countries often extend beyond their geographical borders and affect countries that are not necessarily geographically adjacent to either of the two conflicting parties. This paper examines the geopolitical implications of the Iranian-Israeli cyber war on the Netherlands.

Samenvatting

De snelle ontwikkelingen in moderne technologie en de bijna volledige afhankelijkheid van de meeste landen van deze technologie hebben de economische, politieke en sociale verhoudingen ingrijpend veranderd. Dit komt door de belangrijke rol die deze technologie speelt bij het faciliteren van verkeer en communicatie tussen landen, het verbeteren van samenwerking, het verkrijgen van toegang tot noodzakelijke informatie met de vereiste snelheid en het verhogen van de efficiëntie van internationale economische activiteit tot ongekende hoogten. Technologie is de basis waarop de cyberwereld leeft en bloeit. De cyberwereld is een uitzonderlijke wereld die afwijkt van de traditionele regels van de menselijke wereld waarin we leven, en die zijn eigen regels heeft. Kracht is bijvoorbeeld van nature het tegenovergestelde van zwakte. Hoe sterker iemand wordt, hoe minder zijn zwakheden worden. Dit is vergelijkbaar met de dieren- en plantenwereld. In de

cyberwereld geldt: hoe geavanceerder de cybercapaciteiten van een land en hoe geavanceerder de digitale overheid, hoe meer kwetsbaarheden het heeft.

Dit stelt moderne technologie bloot aan zeer ernstige gevolgen als deze technologie misbruikt of getransformeerd wordt tot een instrument voor politieke en militaire conflicten tussen landen. Dit is in de afgelopen twee decennia gebeurd tussen verschillende landen, met name tussen Iran en Israël. Het conflict tussen deze twee landen in het Midden-Oosten escaleert, en elk land ontwikkelt zijn eigen cybertools en gebruikt deze in de strijd tegen de ander. Omdat cyberconflicten zich afspelen in een niet-geografische ruimte, reiken de gevolgen van een cyberconflict, of cyberoorlog, tussen twee landen vaak verder dan hun geografische grenzen en treffen ze landen die niet noodzakelijkerwijs geografisch grenzen aan een van de twee conflicterende staten

Inhoud

1- Introduction: 5

1.1 Research methodology: 7

1.2 Importance of research: 10

1.2.1 Iranian-Israeli Relations: 10

1.2.2 Dutch-Israeli relations: 12

1.2.3 Dutch-Iranian relations: 14

2- The Cyber War: 18

2.1 The Cyberspace: 18

2.2 The Cyber War: 19

2.3 Features of Cyber War: 21

2.4 The Most Prominent Forms of Weapons Used in Cyber Wars: 22

2.4.1 Logic Bombs: 22

2.4.2 Stuxnet 23

2.4.3 Duqu: 23

2.4.4 Flame: 24

2.4.5 Shamoon: 24

2.4.6 Decoy Dog: 24

2.5 Conclusion: 25

3- The Iranian Cyberspace: 25

3.1 Iranian governmental cyber instiutions: 26

3.1.1 Supreme Council of Cyberspace: 26

3.1.2 National Cyberspace Center: 27

3.1.3 Center to Investigate Organized Crime (CIOC): 27

3.2 Quasi-governmental Institutions: 27

3.2.1 Iranian Cyber Army: 27

3.2.2 The Basij Cyber Brigades: 28

3.2.3 Helix Kitten: 28

3.2.4 The Charming Kitten: 28

3.2.5 Shamoon Group: 29

3.2.6 Mabna Institute Group: 29

3.3 Iran's Cyber Agents: 29

3.3.1 The Syrian Electronic Army: 29

3.3.2 Hezbollah Cyber Factions: 30

3.3.3 Houthi Cyber Group: 30

3.4 Conclusion: 30
4- The Israeli Cyberspace: 30
4.1 The Unit 8200: 32
4.2 the Government Infrastructure for the Internet Age: 32
4.3 Israel National Cyber Directorate: 33
4.4 The Official Authority for Information Protection: 33
4.5 National Cyber Defense Authority: 33
4.6 The Unified Cyber Corps: 33
4.7 The Unit 433: 33
4.8 The Israeli Cyber Dome: 34
4.9 Conclusion: 34
5- The Iranian-Israeli Cyber War: 34
5.1 Conclusion: 37
6- The Implications of the Iranian-Israeli cyber war on the Netherlands: 38
7- Conclusion: 41
8- Bibliography: 43

1- Introduction:

The Middle East has been witnessing complex, dynamic conflicts since the fall of the Ottoman Empire at the beginning of the twentieth century. The collapse of the Ottoman Empire marked the collapse of a stable system of governance that had dominated politics, administration, the economy, and the organization of diverse religious and ethnic communities for four centuries.[1] The collapse of the Ottoman Empire was therefore a structural collapse of the traditional world order in the Middle East. European colonialism, particularly the French and British, replaced the Ottoman Empire in controlling most of the Middle Eastern countries. The French and British divided the Arab region that was under Ottoman rule among themselves, to serve their interests, pursuant to an agreement between the two parties known as the Sykes-Picot Agreement. European rule of the Arab region during the colonial period differed politically and administratively from the rule of local communities, as was the case during the Ottoman period. Each of the French and British attempted, in the areas under their control, to devise hybrid systems of government similar to those in their own countries, on one hand. And on the other hand, they relied on administrative divisions of the territories they occupied based on religious and sectarian lines, serving the interests of the colonizing power, without taking into account the nature of the societies themselves and the major changes that had occurred and continue to occur within these societies as a result of the collapse of the Ottoman Empire.

Most of the countries of the Arab Levant countries gained their independence from European colonialism in the mid-twentieth century. These newly emerging countries faced major challenges, leading to internal conflicts among themselves, such as the demarcation of national borders under Arab regimes vying for control and influence. Each Arab country began to adopt a nation-state mentality regarding its internal borders. Some countries, such as Egypt under Gamal Abdel Nasser, and Syria and Iraq under the Baath Party, embraced the ideas of Pan-Arabism ideology to justified their expansion within the borders of other Arab countries. From here, the Cold War began in the Middle East, particularly between the new republics supported by the Soviet Union, such as Egypt, and the traditional monarchies supported by America, such as Saudi Arabia. During the Shah's reign, Iran, supported by the United States, was not far from the Cold War in the Middle East on the side of the kingdoms, before moving to the side of the republics supported by the Soviet Union after the fall of the Shah and Iran's transformation into a republic.

The most significant and foremost challenge was the declaration of the establishment of the State of Israel in 1947 and the Arabs' entry into a war with Israel in 1948, which they lost. Each country then attempted to blame the other for the loss. In his rewriting of the history of the 1948 war, Israeli historian Avi Shlaim refers to these conditions at the time, represented by internal Arab conflicts among the newly emerging countries over control and influence, each country's fear of the

[1] Albert Hourani, *A History of the Arab People* (Faber & Faber, 2013), 316.

other, and the Arab-Israeli conflict.[2] The Arab-Israeli conflict has been ongoing since the mid-twentieth century. As a result of this conflict, the region has experienced continuous wars, interspersed with periods of calm, truces, and occasional peace treaties between Israel and individual Arab states such as Egypt, Jordan, and more recently, the United Arab Emirates. However, this does not negate the arms race between these states for potential confrontation with each other. On the other hand, the Arab-Arab conflict over borders, influence, and control continues between several neighboring Arab regimes. In 1962, Egyptian President Gamal Abdel Nasser sent his forces to Yemen to fight alongside the armed Yemeni opposition against the Mutawakkilite Kingdom of Yemen, which was supported by Saudi Arabia. In 1976, Syrian President Hafez al-Assad sent his army to occupy Lebanon, which had controlled Lebanon for three decades and only withdrew following a UN resolution. In 1990, Iraqi forces invaded Kuwait.

Since 1979, Iran has strongly entered the arena of the Arab-Arab and Arab-Israeli conflicts, following the victory of the Iranian Revolution and Khomeini's rise to power in Tehran. Khomeini declared hostility toward the West and its interests, not only in Iran but also in the Middle East as a whole. This hostility included the Western camp's allies in the region, represented by Israel and the Arab Gulf states. Iranian-Arab hostility reached the stage of direct military confrontation between Iraq and Iran, which extended from 1980 to 1988. Iran also supported and trained armed militias against existing regimes in other Arab countries, such as the Houthi militia in Yemen, which has attacked Saudi Arabia and Israel more than once, and the Hezbollah militia in Lebanon, which intervened in the Syrian war against the Syrian revolution and the Gulf-backed opposition. In its conflict with Israel, Iran has supported Palestinian organizations, most notably Hamas, while Israel, in turn, supports the Iranian opposition. Turkey has also entered the Middle East conflict since the outbreak of the Syrian revolution in 2011, alongside the Syrian opposition, in the face of Iranian and Russian influence in the region. Turkey has also sought to strengthen its influence in Syria since the fall of al-Assad regime in December 2024, a move Israel strongly opposes and which has exacerbated tensions between Israel and Turkey.

Thus, The Middle East has been witnessing intense conflicts since the beginning of the twentieth century. These conflicts have become increasingly complex and intense over time, often escalating into military conflicts. In light of this situation, Middle Eastern countries are racing to equip their armies and acquire, develop, and innovate modern military armaments. Modern technology and cyber tools play a significant role in these conflicts and wars. Traditional tools, such as massive human recruitment and heavy military equipment, are no longer sufficient to resolve any military conflict. A prime example of this are the Israeli pager attacks against Hezbollah, which killed dozen of its elite fighters with the push of a remote button and significantly weakened the group. This is a more effective outcome than what is required in conventional military wars, which can extend for months or years, exhausting both sides without achieving a military victory.

In addition to the direct political conflict between Iran and Israel and the military conflict Iran is waging with Israel in shadow, the two countries have been waging a cyber war for more than two

[2] Avi Shlaim, “Israel and the Arab Coalition in 1948,” In *The War for Palestine: Rewriting the History of 1948*, ed. Avi Shlaim and Eugene L. Rogan, (Cambridge University Press, 2012), 80.

decades. Israel and Iran are the two most advanced cyber powers in the Middle East. Each is developing its cyber knowledge and weapons to confront the other. Because cyberspace is not geographically defined and attackers often cannot be tracked, the effects of this confrontation between Iran and Israel sometimes extend to their allies, as Israel did when it attacked Hezbollah using pagers, and as Iran did when it attacked the American Saudi company Aramco in Saudi Arabia in 2012. Because the Netherlands has ties with several countries in the Middle East, it is not immune to the impact of the complex conflict in the East. As for Israel and Iran, the Netherlands has a special relationship with Israel that extends to cooperation in the field of technology and cybersecurity, and a relationship of complex standing with Iran that has witnessed significant progress at times and decline at many times. This places the Netherlands at the heart of the Iranian-Israeli cyber war. This paper examines the geopolitical implications of the Israeli-Iranian cyber war on the Netherlands.

There has been several research written in recent years about the cyber war between Iran and Israel. For example, in his Arabic-language book "Elctronic War" Egyptian military researcher Faisal Abdul Ghaffar presents the confrontation between Iran and Israel as an example of fourth-generation war, or cyber war. Tikrit University researchers Hiba Alnasiry and Muthanna Merei also examined Iranian and Israeli cyber institutions in their research on cyber institutions in the Middle East. Professor Gawdat Bahgat also provided an extensive chapter on the cyber confrontation between Iran and Israel in his book, co-authored with Anoushiravan Ehteshami and published by Cambridge University Press, entitled: "Defending Iran: From Revolutionary Guards to Ballistic Missiles". Veronika Netolická and Miroslav Mares, two researchers from the University of Masaryk Universiteit Brno, presented a study on the arms race in cyberspace, taking Iran and Israel as a study case. What my research adds in this regard is examining the geopolitical implications of the Iranian-Israeli cyber war on the Netherlands.

To answer the research question: **What are the geopolitical implications of the Israeli-Iranian cyber war on the Netherlands**, this paper is divided into five main chapters. Chapter 1 examines the nature of cyberspace, the meaning of cyber war, and its advantages compared to conventional war. Chapter 2 examines the Iranian cyberspace, and Chapter 3 examines the Israeli cyberspace. Chapter 4 examines the Iranian-Israeli cyber war and the mutual attacks between them over the past two decades. Chapter 5 examines the geopolitical implications of the Iranian-Israeli cyber war on the Netherlands.

1.1 Research methodology:

Before delving into the research methodology I will follow in this paper, I will highlight two important points: the sources I relied on and my experience and research capabilities to carry out this paper. The topic this paper addresses connects two completely different worlds: the geopolitical world, which is based on an analysis of clear historical and current facts, such as Dutch-Israeli relations and Dutch-Iranian relations, for example. When researching this issue, researchers usually encounter no difficulties in finding clear and reliable sources. The second world is the cyber world, a virtual world shrouded in much mystery, both regarding the methods of carrying out attacks and the tools used, and regarding the attacking and defending states, which develop and use their cyber tools with great secrecy. Regarding this issue, the research sources

available to me were very limited, and many of them relied on news reports. I, in turn, relied on collecting numerous media reports, comparing them, and analyzing them to arrive at the closest possible image of my research objective.

Because media reports are not reliable academic sources, I used them for specific purposes, such as obtaining a news, media report, or investigative report that had not been refuted by the relevant stakeholders. For example, I compared a Reuters news report about cyber-attacks on Aramco with a Guardian and BBC report on the same news. I also reviewed the same news on the Saudi Press Agency. In other words, I verified the same news from several reliable media outlets, and ultimately sourced the story from Reuters because Reuters reported it without any analysis or accusations at the time, which was exactly what I wanted to achieve. However, when the US intelligence pointed the finger at Iran, I did not limit myself to media reports; rather, I confirmed the story through an official source whose name was clearly mentioned in the New York Times rapport.

Finally, this paper, as it examines the geopolitical implications of cyber war, can be applied to both the humanities and social sciences—political science, history, Jewish studies, or Iranian studies. In my case, this paper serves as a master's thesis in Jewish studies at the University of Amsterdam, and will also be used at the Center for Information Security and Privacy Protection in the Netherlands.

For this paper, I relied on sources in three primary languages, which I am fluent in. English-language sources contain extensive studies and researchs on historical Iranian-Israeli relations, as well as a wealth of English-language news reports and media investigations on the mutual cyberattacks between Iran and Israel. Dutch-language sources contain numerous sources on the importance of global cybersecurity and the extent of Iranian threats to the Netherlands and other countries. Military and civilian intelligence regularly assess the Dutch cybersecurity situation and the most significant threats facing the Netherlands and global cybersecurity. The State Cybersecurity Council (Cyber Security Raad) also conducts regular assessments to advise the government on its future cybersecurity strategy. Several government centers collaborate to disseminate information, raise awareness, and share expertise regarding global and local cyberthreats, including the Center for Information Security and Privacy Protection (CIP), the National Cyber Security Center (NCSC), and the National Coordinator for Counterterrorism and Security (NCTV). Furthermore, the paper examines the development of Dutch-Israeli and Dutch-Iranian relations, where many sources can be found in Dutch.

As for the Arabic language, its importance stems from its abundance and modernity, particularly in light of the mutual cyberattacks between Iran and Israel. Many Arab countries are subject to cyberattacks from both Iran and Israel, making cybersecurity a focus of interest for many Arab countries, particularly Saudi Arabia and Egypt. Spending on cybersecurity in Saudi Arabia for 2023 exceeded $3 billion, and the number of cybersecurity specialists in Saudi reached 19,600.[3] The National Cybersecurity Authority in Saudi Arabia develops government and community awareness programs through the Mobile Cybersecurity Exhibition, a traveling exhibition that travels

[3] “Cyber Industry Development”, National Cybersecurity Authority, https://nca.gov.sa/ar/.

throughout the year from one government agency to another, targeting both employees and citizens. It also organizes awareness sessions, workshops, and training for government employees across various sectors, in addition to issuing periodic studies and reports on local and international cybersecurity.[4] As for Egypt, in 2014 Egypt established the Supreme Council for Cybersecurity with the aim of protecting the country's cyberspace, enhancing cybersecurity, promoting cyber awareness, enhancing cooperation with the private sector and non-governmental institutions working in cybersecurity, and promoting regional and international cooperation to unify efforts to confront cyber threats.[5]

The second issue I would like to address is my academic capabilities and practical experience in researching such a topic, particularly in terms of linking and analyzing what is political and historical on the one hand, and what is technological and cyber on the other. In this paper, I wish to utilize all my capabilities and previous experience, which I gained through my studies at the University of Amsterdam of Middle Eastern and Jewish Studies. This experience has provided me with strong research skills in the Middle East and the decades-long conflicts there, particularly the Arab-Israeli conflict, the Arab-Iranian conflict, and the Israeli-Iranian conflict. This is in addition to my personal knowledge of the region, having come from there, and my previous political interest, which I developed at the Faculty of Law at the University of Damascus in Syria, before witnessing the Syrian revolution and following all the complexities and regional conflicts it witnessed. My experience and knowledge of technology and cybersecurity are the result of my work at the Center for Information Security and Privacy Protection in the Netherlands from 2020 until the date of this research. Over the past five years of my work at the Center, I have gained significant expertise in the field of cybersecurity. This expertise stems from my reading of dozens of government documents and viewing hundreds of hours of videos on government cybersecurity experiences in the Netherlands at various levels, starting with the central government and the parliament, both chambers, then ministries, independent government agency, provinces, and municipalities, in addition to the expertise of the health sector in this field. I have also attended numerous cybersecurity conferences, both those I co-organized with my colleagues at the Center and those organized by our government partners. I have also completed several training courses in information security, risk assessment, and project management related to government cybersecurity.

As for the research approach I follow in conducting this paper, in the first chapter, I adopt a descriptive approach to explain the meaning of cyber war. In this chapter, I will seek to compare different definitions of cyber-related concepts such as cyberspace, cybersecurity, and cyber war. I will then discuss the characteristics of cyber war, clarifying its difference from conventional war. Finally, I will discuss the most prominent types of weapons used in cyber war. I will also adopt a descriptive approach to research the Iranian cyberspace, which consists of official government institutions, Quasi-governmental institutions affiliated with the Islamic Revolutionary Guard Corpss (IRGC) without official recognition, and cyber agents in the Middle East. I will use the same

[4] National Cybersecurity Authority, “Cyber Knowledge.”

[5] “Prime Minister’s Decree No. 2259 of 2014”, The Cabinet of Ministers: The Egyptian Supreme Cybersecurity Council (ESCC), https://www.escc.gov.eg/page1_1_en.html.

approach to research the Israeli cyberspace, which consists of several government institutions. I will also examine how Israel develops its cyber capabilities through international partnerships and cooperation, particularly joint training exercises with the US military. As for the fourth chapter, which examines the Iranian-Israeli cyberspace, I will adopt a descriptive historical approach. Finally, I will adopt an analytical approach to analyse the impact of the Iranian-Israeli cyber war on the Netherlands.

1.2 Importance of research:

The Netherlands is one of the advanced countries that manufactures and produces modern technology. It relies entirely on cyberspace to manage its infrastructure and various state facilities, along with the private sector, which contributes significantly to the local economy. As mentioned above, the more technologically advanced a country becomes, the greater its cybersecurity risks. Therefore, the Netherlands pays special attention to its cybersecurity. To enhance this security, its experts must keep an eye on cyberspace, not only to enhance its own cybersecurity, but also to evaluate and learn lessons from other countries' conflicts in this space. Although the Netherlands is geographically distant from both Iran and Israel, it is at the heart of their geopolitical conflict and is affected by the cyberstorm of both parties, due to its complex historical and political ties with both parties, both as an independent state and as a member of the European Union and NATO. To demonstrate the practical significance of the research question, which will focus on the geopolitical implications of the Israeli-Iranian cyber war on the Netherlands, we must begin by discussing Iranian-Israeli, Dutch-Israeli and Dutch-Iranian relations.

1.2.1 Iranian-Israeli Relations:

The relationship between Iran and Israel has not always been as hostile as it is today. Iran was the second Muslim-majority country to recognize Israel after its founding in 1948 (Turkey was the first Muslim-majority country to recognize Israel). Iran's relationship with Israel strengthened after the successful coup against Iranian Prime Minister Mohammad Mosaddegh in 1953, who had previously accused Israel of subservience to the United States and Britain and of plotting a coup against his government. The coup against Mossadegh strengthened the power of the Shah, Mohammad Reza Pahlavi, who had close ties with Britain and America and admired Israel.[6]

Iran was fearful of the spread of Arab nationalism, led by Gamal Abdel Nasser and supported by the Soviet Union. Therefore, it was in Iran's interest to maintain its relations with Israel. Indeed, during the Shah's reign, relations between Israel and Iran were strategic and reciprocal, given the threat posed by both countries' Arab adversaries. On the Israeli side, the Arabs were calling for a comprehensive war to completely eliminate Israel and liberate Palestine. On the Iranian side, they were resentful of Arab nationalist aspirations and the struggle to change the name of the Persian Gulf to the Arabian Gulf.[7] Despite the strategic ties that linked the Shah to Israel, this did not

[6] Nora Maher, “Balancing deterrence: Iran-Israel relations in a turbulent Middle East,” *Emerald Publishing Limited* 8, no. 3 (2023): 227.
[7] Ibid, 228.

prevent him from criticizing Israel after its 1967 war with the Arabs, for fear of arousing Muslim sensitivities against his rule.[8]

Eventhough, the Shah continued, carefully, to cooperate with Israel. In the 1970s, Iranian-Israeli economic cooperation led to the establishment of new companies, particularly in the oil sector. To conceal these partnerships, the companies were established in Switzerland and Panama, under a central legal entity known as the Trans-Asiatic Oil Company. Iranian oil pipelines covered Israel's oil needs. In contrast, Israeli investments have greatly strengthened the Iranian economy. In 1977, a joint Iranian-Israeli military project called "Project Flower" focused on the development of advanced missile systems. It was one of six oil-for-arms contracts that Iran and Israel signed in the late 1970s.[9]

After the fall of the Shah's regime and Ayatollah Khomeini's rise to power in Iran, the relationship between Iran and Israel shifted to open hostility as a result of Iran's shifting ideology. Iran sought to Islamize the Arab-Israeli conflict, with Khomeini's vision being that it was a struggle to liberate holy sites and Islamic lands, and that the struggle to liberate Palestine was a jihad in the path of God and a duty for all Muslims.[10] Among the principles Khomeini promoted was a focus on resisting Western hegemony over the Arab and Islamic region. He imposed a civilizational clash with the West and considered Israel to be the "Little Satan," performing the duties of the "Great Satan," the United States, in the region. He also considered the Arab states allied with the United States to be apostates from Islam.[11] Thus, Khomeini forcefully brought Iran into the Cold War arena in the Middle East, but through the gateway of Islamic ideology.

When the Iran-Iraq war broke out in the 1980s, the Iranian regime found itself in the same position as the former Shah's regime, needing to cooperate with Israel to confront the Arabs, Iraq led by Saddam Hussein and behind him the Gulf Cooperation Council countries. Here, Iran began to restore a kind of low-level relationship with Israel. Israel also found Iran's political and military support in its interest, based on the principle that the enemy of my enemy is my friend. In the early 1980, Israeli Prime Minister Menachem Begin persuaded the United States to allow Israel to circumvent the arms embargo on Iran, enabling Israel to supply Iran with fighter jets and other weapons to confront Iraq. In return, Khomeini allowed large numbers of Iranian Jews to leave for the United States and Israel.[12]

Cooperation between Israel and Iran ceased in the 1990s, but Israel did not view Iran as a direct threat at the time. The threat from Saddam Hussein's Iraq was prioritized. However, the Israeli security establishment's concern about Iran began to grow after the latter developed ballistic weapons with a range that could reach Israel. On the other hand, after the end of the Iran-Iraq War, Iran began to pay greater attention to its nuclear program. This prompted Israeli politicians to

---

[8] Dalia Dassa Kaye, Alireza Nader and Parisa Roshan, "A Brief History of Israeli-Iranian Cooperation and Confrontation," in *Israel and Iran: A Dangerous Rivalry,* (RAND Corporation, 2011), 9.

[9] Ibid, 14.

[10] Gawdat Bahgat, "Iranian-Israeli Confrontation: The Cyber Domain," *Middle East Policy, Vol. XXVII*, no. 3 (2020): 116.

[11] Maher, "Balancing deterrence: Iran-Israel relations in a turbulent Middle East," 228.

[12] Dalia Dassa Kaye, Alireza Nader and Parisa Roshan, "A Brief History of Israeli-Iranian Cooperation and Confrontation," 15.

reassess the threat Iran poses to Israeli national security.[13] In the early 2000s, competition between Israel and Iran began to intensify after the two sides eliminated their common enemy, Saddam Hussein, in Iraq, and the Taliban, which posed a threat to Iran at the time, was defeated in Afghanistan. Tensions between the two countries were exacerbated by the rise to power of Mahmoud Ahmadinejad in Iran in 2005, who harshly criticized Israel and denied the Holocaust. In 2006, Iran supported its ally Hezbollah in its war with Lebanon, and it did the same with Hamas in the 2008 and 2012 wars, and the most recent war in Gaza since October 2023.[14] Iran's direct intervention in the Syrian civil war from 2011 on the side of Bashar al-Assad until the fall of his regime in late 2024 was an additional factor in increasing tensions between Israel and Iran, leading to direct military confrontation at times in Syria.

1.2.2 Dutch-Israeli relations:

The Netherlands was one of the last European friends to recognize Israel after the declaration of the nascent state in 1948. This was because the Netherlands at the time was still trying to regain control of the Dutch East Indies, and the government in The Hague believed it was unwise to insult the Muslim population of its most valuable colony by supporting the Zionists against Arab claims to Palestine. The Netherlands did not formally recognize the Jewish state of Israel until after the final defeat of Indonesia in December 1949. Against the backdrop of the Cold War and the decision of Israel's first prime minister, David Ben-Gurion, to join the Western camp, Dutch Prime Minister Willem Drisse of the Labour Party began strengthening Dutch relations with Israel. Moreover, the Cold War was accompanied by ideology led to polarization and rapprochement between the social democratic parties in the Netherlands and the Israelis counterparts.[15]

Socially, the outbreak of the Six-Day War in 1967 coincided with a time when guilt over the Holocaust clearly defined Dutch society's attitude toward Israel. The massive support for Israel during the Six-Day War came at a time when Dutch society was undergoing a reassessment of its wartime past, prompted by the trial of Adolf Eichmann in Jerusalem. This included the screening of a popular documentary series about the Nazi occupation on national television and the publication of new books about the Holocaust.[16]

Opinion polls conducted by the Netherlands Institute for Public Opinion (NIPO) immediately after the 1967 war showed that 67% of the Dutch public sympathized with Israel, a higher percentage than in other Western European countries (the United Kingdom 59%, France 57%, and the United States 55%). Respondents most frequently cited the Holocaust as a direct reason for supporting Israel. This popular support began to decline after the 1967 war, falling from 67% in 1967 to 51% in 1969, then to 37% in 1974, followed by a temporary increase to 57% in 1979, and then declining again to 35% in 1982.[17] In a recent opinion poll conducted by the Dutch Ipsos

[13] Ibid, 16.
[14] Ibid, 17.
[15] Frederik Grünfeld, *Nederland en het Nabije Oosten. De Nederlandse rol in de internationale politiek ten aanzien van het Arabisch-Israelisch conflict 1973-1982,* (Deventer: Kluwer, 1991), 53.
[16] Peter Malcontent, "The Netherlands, the EU and the Israeli-Palestinian Conflict", *European Review of International Studies*, no. 9 (2022): 274.
[17] Malcontent, "The Netherlands, the EU and the Israeli-Palestinian Conflict," 275.

organization in October 2024, it was shown that nearly half of the Dutch people believe that the Dutch government should be more critical of Israel.[18]

Returning to the governmental level, although the Dutch government criticized Israel's occupation of the West Bank and Gaza after the 1967 war, it simultaneously supported Israel financially and militarily in its 1973 war with the Arabs. The Netherlands immediately responded to Israel's request for material support for the Israeli war effort. The Arab oil embargo on the Netherlands due to its support for Israel did not deter the Dutch government from backing down and opening Dutch arms depots to Israel. Feelings of remorse among Dutch politicians again played a significant role in this war. Then-Dutch Defense Minister Henk Vredeling expressed this by saying, "I saw the Jews retreating again. I couldn't prevent it," meaning he was unable to withhold arms from Israel. In 2012, Foreign Minister Uri Rosenthal of the Conservative Liberal Party refused to endorse a joint European statement that cited a European Union report criticizing the Israeli occupation regime in the West Bank. Rosenthal remained steadfast in the face of unanimous criticism from the Germans, French, and British.[19] Following Hamas's attack on Israel on October 7, 2023, the Dutch government announced its full support for Israel, through its then Prime Minister, Mark Rutte.[20] The government's position received broad support from the Dutch Parliament.[21] The Dutch government continues to support Israel despite international and European criticism of Israel's violent response to Hamas during its war on Gaza, which has killed tens of thousands of civilians.

In addition to the political, governmental, and social relations between the Netherlands and Israel, there are economic relations and military cooperation between the two countries. The Israeli embassy issued a statement on October 1, 2024, marking the 75th anniversary of friendship and diplomatic relations between the Netherlands and Israel. In its statement, the embassy emphasized the depth of relations between the two countries, which are based on several aspects, including trade and scientific exchange.[22] The Dutch Ministry of Foreign Affairs also points out on its website the depth of relations between the two countries and cooperation in various fields, including economy, technology, and cybersecurity[23], which is the subject of our research. The Netherlands primarily exports to Israel electronic devices, medical equipment, vehicle spare parts, information technology, and scientific research equipment. The Netherlands imports vegetables, fruits, crude oil, electronic devices, and scientific research equipment from Israel. Trade between the two countries reached €4.7 billion in 2023.[24] In the military field, the Defense Department at

---

[18] Maartje van den Koppel and Peter Kanne, *Opinieonderzoek Israël-Palestina*, (Ipsos I&O, 2024), chap. 2, https://www.ipsos-publiek.nl/wp-content/uploads/2024/10/opinieonderzoek-israel-palestina-definitief.pdf.
[19] Malcontent, "The Netherlands, the EU and the Israeli-Palestinian Conflict," 276.
[20] "Premier Rutte: Nederland staat achter Israël," *NOS*, October 7, 2023, https://nos.nl/collectie/13959/video/2493198-premier-rutte-nederland-staat-achter-israel.
[21] "Brede steun Tweede Kamer voor kabinetsstandpunt: Israël heeft recht op zelfverdediging," *NOS*, October 10, 2023, https://nos.nl/collectie/13959/artikel/2493597-brede-steun-tweede-kamer-voor-kabinetsstandpunt-israel-heeft-recht-op-zelfverdediging.
[22] "The Netherlands and Israel: a close friendship," *Embassy of Israel The Hague*, November 01, 2024, https://new.embassies.gov.il/netherlands/en/the-embassy/bilateral-relations.
[23] "The Netherlands and Israel," *Political department and press-related affairs*, https://www.netherlandsandyou.nl/web/israel/about-us/who-we-are/political-department.
[24] "Rijksdienst voor Ondernemend Nederland, Handel Nederland – Israël," *Rijksoverheid*, October 2023, https://www.rvo.nl/onderwerpen/landen-en-gebieden/israel/handel.

the Dutch Embassy in Tel Aviv is responsible for bilateral military cooperation.[25] There is no official, precise information available about the extent of military, technological, and intelligence cooperation between the two countries, but it can be concluded from some facts that it is at the highest levels. An investigation by the Dutch newspaper Volkskrant in early 2024 revealed that a Dutch agent was the one who planted the Stuxnet virus at Iran's Natanz nuclear facility in 2007. This operation, which sabotaged a significant portion of Iran's nuclear program, was the result of a complex intelligence operation between Israeli intelligence and its American and Dutch counterparts.[26] On February 12, 2024, the Supreme Court in The Hague decided that the Netherlands must stop exporting F-35 spare parts to Israel.[27] This means that the Supreme Court has suspended existing military cooperation between the Netherlands and Israel, the Netherlands' most prominent ally in the East. As discussed above, the two countries enjoy strong historical, social, political, and economic relations, leading to cooperation in various fields, not least defense and technology.

1.2.3 Dutch-Iranian relations:

On the other side, the current relationship between Iran and the Netherlands is marred by underlying hostility. To understand the nature of this current hostility, one must understand Iranian-Dutch relations since the 1960s. The Netherlands and Iran have enjoyed strong economic relations for centuries, as Iran was an important center for Dutch trade in the East since the founding of the Dutch East India Company in the early 17th century. In the modern era, particularly during the Shah Mohammad Reza Pahlavi's reign, Iranian-Dutch relations developed significantly due to the Shah's development of relations with the West in general. After World War II, British influence in Iran declined and the power of the United States grew, supporting the Shah to remain in power. Although the country prospered during the Shah's reign, the lower classes did not benefit from this prosperity. The Shah also began to lean toward a repressive dictatorship, abolishing the multiparty system and imprisoning and executing opponents. There was also societal rejection of the growing influence of America, capitalism, and the associated Western morals.[28]

Shah visited the Netherlands in 1959, and after this visit, Dutch companies participated in non-commercial trade concessions in Iran. This visit opened up an important investment opportunity for the Netherlands. Keen to maintain a distinguished relationship with Shah, the Netherlands thus avoided his tyranny and repression of Iranian opponents of his rule.[29] When the Iranian revolution broke out in Tehran against the Shah, the center-right-wing Dutch government expected that the Shah would be able to control the revolution thanks to American support and the support of his army. The Dutch left, however, expected that the revolution would end the monarchy in Iran and

[25] "Defence department, The Netherlands and Israel," *Rijksoverheid*, https://www.netherlandsandyou.nl/web/israel/about-us/who-we-are/defence-department.
[26] Huib Modderkolk, "Sabotage in Iran," *De Volkskrant*, January 08, 2024, https://www.volkskrant.nl/kijkverder/v/2024/sabotage-in-iran-een-missie-in-duisternis~v989743/.
[27] "Levering F-35 onderdelen aan Israël in strijd met Gemeenschappelijk Standpunt EU en Wapenhandelsverdrag?," *Gerechtshof Den Haag*, December 12, 2024, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHDHA:2024:191.
[28] Marjolein Koster, "Waarom is de relatie tussen Iran en het Westen zo moeizaam?," *NPO Kennis*, August 20, 2024, https://npokennis.nl/longread/7780/waarom-is-de-relatie-tussen-iran-en-het-westen-zo-moeizaam.
[29] Maaike Warnaar, *Onze vriend op de pauwentroon*, (Amsterdam University Press, 2023), 16-17.

replace it with a democratic system.[30] The Dutch right supported the Shah against the popular revolution, while the Dutch left supported the Iranian left, which ended up out of power during the Khomeini era.

Dutch embassy staff, businesspeople, and companies in Tehran were getting their information about the internal situation from Iran's financial elite, who were aligned with the Shah. Consequently, the Dutch government was informed that there was no doubt about the Shah's survival. The Dutch government remained on the Shah's side until the last moment, and because it did not expect the Shah to fall, it did not open any channels of communication with his opponents, who later assumed power.[31] Iranian relations with the West in general, and with the United States in particular, deteriorated significantly after Khomeini came to power in 1979. There were widespread suspicions of Western spying and attempts to control Iran. Iran's new policy negatively impacted relations with the Netherlands. From its first days, the new Iranian government began canceling trade deals with the Netherlands and suspending Dutch companies from operating in Iran.[32]

In 2006, the United Nations imposed sanctions on Iran over suspicions of its uranium enrichment program. Since the hardline conservative Ahmadinejad came to power in Iran, the West has feared that the country was developing nuclear weapons. In the years that followed, sanctions were imposed, including an arms embargo, and banks were cut off from international traffic. In 2010, the European Union followed the UN's lead by imposing an embargo on Iranian oil and gas trade and on Iran's nuclear industry, and later on financial transactions were also banned. As a result of these sanctions, the Iranian currency (the rial) has plummeted, and the country has become economically isolated. Since the Netherlands is part of the EU that imposes sanctions on Iran, Dutch-Iranian relations continue to be negatively affected.

Because the continuation of this situation negatively impacts Iran and the Iranian economy, former Iranian President Hassan Rouhani began negotiations in 2015 to conclude a nuclear agreement. This led to an agreement with the international community (Germany, France, the United Kingdom, the United States, Russia, and China) on July 14, 2015, with the exception of Israel. Although the agreement stipulates that Iran will halt construction of nuclear facilities and reduce uranium enrichment, Israel remains concerned about Iran's ability and desire to acquire nuclear weapons.[33] In the same year, Dutch Foreign Minister Bert Koenders visited Tehran. This visit was significant because the Netherlands held the European Union presidency in 2015, and it was the first visit by a Dutch foreign minister since 2001. Koenders explained that this visit would not have been possible had Iran not reached a nuclear agreement with world powers. At the end of the visit, the Dutch foreign minister held a press conference with his Iranian counterpart, Mohammad Javad Zarif, who emphasized his country's desire to restore good relations with the Netherlands and that Tehran could present a good opportunity for Dutch companies operating in the oil and gas industry, as well as those wishing to invest in the agricultural and water sectors. It is worth noting that the Iranian

[30] Ibid, 210.
[31] Ibid, 227.
[32] Ibid, 223.
[33] Koster, “Waarom is de relatie tussen Iran en het Westen zo moeizaam?”.

foreign minister praised the historical Dutch-Iranian relations, which span four centuries, but the relationship has been somewhat negative in recent decades.[34]

During 2016, the two countries exchanged several high-level delegations, including visits by Foreign Minister Mohammad Javad Zarif, Vice President and Head of Cultural Heritage Dr. Zahra Ahmadipour, and the Minister of Agriculture to the Netherlands. The Minister of Economic Affairs and the Minister of Infrastructure and Environment also visited Iran, accompanied by hundreds of companies, which achieved positive results in both countries. In 2017, the Iranian Embassy in The Hague held a grand ceremony to mark the 38th anniversary of the victory of the Iranian Revolution. The ceremony was attended by high-ranking Dutch political figures, who were welcomed by Iranian Ambassador Alireza Jahangiri. The Iranian ambassador expressed the strength of the relationship they have built with the Netherlands, particularly highlighting the new phase of their historical relations over the past three years, especially with the Netherlands leading Europe as Iran's largest trading partner in the European Union as of 2016.[35]

Since mid-2018, Iranian-Dutch relations have deteriorated again and witnessed significant tensions. In June 2018, the Dutch Foreign Ministry expelled two employees of the Iranian embassy in The Hague, following accusations that employees of Iranian embassies in European countries were involved in planning bombings targeting an Iranian opposition meeting in the French capital, Paris.[36] Iran then rejected European accusations that its embassy staff were involved in planning bombings on European soil and accused the Netherlands of seeking to obstruct nuclear negotiations with world powers, following the United States' withdrawal from the agreement. In September of the same year, during a military parade in the southern Iranian city of Ahwaz commemorating the Iran-Iraq War (1980-1988), four attackers disguised as members of the Islamic Revolutionary Guard Corps opened fire on the parade participants. The attack killed approximately 29 people, most of them soldiers, and wounded dozens.[37] Iran accused the Ahwazi resistance, a separatist movement calling for the secession of the southern Ahwaz region from Iran, of carrying out the attack. Among the groups affiliated with the separatist movement is the Arab Struggle Movement for the Liberation of Ahwaz, most of whose members reside in the Netherlands, Denmark, and the United Kingdom. Accordingly, Tehran summoned the ambassadors of the aforementioned countries, accusing them of providing shelter and support to members of the separatist movements that Iran accuses of the attack.[38] Sven Koopmans, a member of parliament for the People's Party for Freedom and Democracy (VVD), who serves as foreign affairs spokesman,

[34] "Iran: relatie met Nederland herstellen," *RTL*, September 20, 2015, https://www.rtl.nl/buitenland/artikel/863021/iran-relatie-met-nederland-herstellen.
[35] "Celebrations for Iran and their Prosperity with The Netherlands," *Diplomat Affairs Magazine*, 2017, https://www.diplomataffairs.nl/celebrations-for-iran-and-their-prosperity-with-the-netherlands/.
[36] "Twee medewerkers Iraanse ambassade het land uitgezet," *AD*, July 06, 2018, https://www.ad.nl/binnenland/twee-medewerkers-iraanse-ambassade-het-land-uitgezet~a4b552ccf/?referrer=https%3A%2F%2Fwww.google.com%2F.
[37] Matthijs van Schie, "Na de aanslag: 4 vragen over conflict Nederland-Iran," *EW*, September 24, 2018, https://www.ewmagazine.nl/verhaal-van-de-dag/achtergrond/2018/09/na-de-aanslag-4-vragen-over-conflict-nederland-iran-645716/.
[38] Schie, "Na de aanslag: 4 vragen over conflict Nederland-Iran.

tweeted that he was outraged by Iran's accusations against the Netherlands. "A terrible attack, very sad. But should we blame the Netherlands?"[39]

In 2022, a government report issued by the Dutch Ministry of Foreign Affairs, assessing the situation in Iran from February 2021 to March 2022, noted a decline in the Iranian economy as a result of the United States' withdrawal from the nuclear agreement and the position of the International Atomic Energy Agency, which stated that Iranian authorities were restricting the work of its inspectors, leading to the return of some economic sanctions on Iran. The report also spoke of the fragility of the internal situation in Iran as a result of popular protests demanding economic and political reform. The report also pointed to Iran's deteriorating political relations with Western countries, particularly the United States. The report also stated that Iran is exposed to cyber attacks as a result of its involvement in regional and international conflicts and its use of similar methods.[40] In 2022, a joint report by Dutch military intelligence (MIVD), civilian intelligence (AIVD), and the National Center for Countering Extremism (NCTV) ranked Iran as the country that poses the highest cyber threat to the Netherlands and its infrastructure.[41]

On April 25, 2025, the Iranian Ministry of Foreign Affairs summoned the Dutch ambassador to Tehran to protest a Dutch intelligence report accusing Iran of killing Iranian citizens in the Netherlands. The report also warned of cyberattacks from Iran (along with Russia, China, and North Korea). The report also states that Iran has recently developed a cyber defense program called "hack-and-leak", where sensitive information is stolen from someone and then posted online in order to harm that person.[42] Relations between Iran and the Netherlands have been increasingly tense due to the two countries' ambivalent stances on the Gaza War since October 2023, with the Netherlands supporting Israel, while Iran stands with Hamas and Hezbollah.

This brief overview of the nature of Dutch-Israeli and Dutch-Iranian relations and their development over the past decades reveals the importance of studying the geopolitical implications of the Israeli-Iranian cyber war on the Netherlands. The Netherlands classifies Iran as a top cyber threat, alongside Russia and China. This is due to the nature of the relationship between the Netherlands and Iran since the 1980s, which included diplomatic attempts to break the ice between the two countries, but these attempts failed. On the other side, the historical Dutch-Israeli relations, dating back to the 1950s, have remained stable throughout these decades and have resulted in Dutch social, political, and military support for Israel since its founding. This relationship between the Netherlands and Israel also results in cooperation between the two countries in all fields, particularly economic, scientific, military, intelligence, and cyber cooperation. The nature of the relations between the Netherlands and both countries and their development in the modern era place the Netherlands at the heart of the Iranian-Israeli cyber war.

---

[39] Schie, "Na de aanslag: 4 vragen over conflict Nederland-Iran.

[40] "Algemeen ambtsbericht Iran van mei 2022," *Rijksoverheid*, May 31, 2022, https://www.rijksoverheid.nl/documenten/ambtsberichten/2022/05/31/algemeen-ambtsbericht-iran-van-mei-2022.

[41] "Dreigingsbeeld Statelijke Actoren 2," *AIVD, MIVD and NCTV*, November 28, 2022, https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2.

[42] "Iran roept Nederlandse ambassadeur op het matje na AIVD-rapport over liquidatiepogingen," *NOS*, April 24, 2025, https://nos.nl/artikel/2564953-iran-roept-nederlandse-ambassadeur-op-het-matje-na-aivd-rapport-over-liquidatiepogingen.

2- The Cyber War:

In order to answering the research question about the geopolitical implications of the Iranian-Israeli war on the Netherlands, it is important to define what cyber war is and how it differs from conventional war. In this chapter, I seek to clarify some concepts related to cyberworld, such as cyberspace, cybersecurity, and cyber war. In the absence of definitive official international definitions of cyber concepts, I will compare several relevant definitions, but whose definitions do not rise to the level of official international definitions. I will then attempt to clarify the differences between these various definitions. I will then address the characteristics of cyber war, clarifying its distinction from conventional war. Finally, I will discuss the most prominent types of weapons used in cyber war. In this chapter, I will rely on institutional sources to explore the definition of cyberspace and cyberwar, including the definitions of the United Nations, NATO, and the Dutch Cyber Dictionary, in addition to academic sources, such as the definition by Michiel Foulon and Gustav Meibauer, researchers at the Center for Security Studies at the Swiss Federal Institute of Technology in Zurich in their research entitled "How cyberspace affects international relations: The promise of structural modifiers." and the definition of the Former White House advisor Richard Clarke and the definition of James Andrew Lewis, director of the Technology and Public Policy Program at the Center for Strategic and International Studies in Washington.

2.1 The Cyberspace:

There is no universal, comprehensive definition of cyberspace, and many cyber-related terms, such as cybersecurity, cyber conflict, cyber war, cybercrime, cyberterrorism, and other terms circulated in the media and politics, are used in different contexts. Because the United Nations and other relevant international bodies have yet to address this issue conclusively, many countries provide definitions of cyberspace based on their own national concepts and needs. The United Nations defines cyberspace as the invisible virtual environment for electronic communications and the electronic environment facilitated by the Internet, which is the most common type of cyberspace.[43] We find this definition inadequate as the United Nations refers its definition of cyberspace to the Internet, which is a form of cyberspace, not the cyberspace. The NATO Cyber Defence Centre defines cyberspace as the set of interconnected, time-dependent information systems and the human users who interact with these systems.[44] The Dutch cyber dictionary defines cyberspace as an ecosystem of digital (networked) technologies, where all kinds of different actors create, store, exchange, use and share information.[45] The National Cybersecurity Authority in the Saudi Arabia goes beyond defining cyberspace, and replaces it with a definition of cybersecurity, as the protection of networks, information technology systems, operational technology systems and their components, including hardware and software, the services they provide, and the data they contain, from any hacking, disruption, modification, entry, use, or illegal exploitation. This concept also includes information security, electronic security, digital security, and the like.[46]

[43] "UN E-Government Knowladgebase," *United Nations*, February 10, 2024, https://shorturl.at/CZ8zr.
[44] Peeter Lorents and Rain Ottis, "Cyberspace: Definition and Implications," *CCDCOE*, https://shorturl.at/jofZd.
[45] "Het cybersecurity woordenboek," *Cyberveilig Nederland*, November 01, 2024, https://shorturl.at/P5jXE.
[46] National Cybersecurity Authority, "Cyber Knowledge."

From an academic perspective, Michiel Foulon and Gustav Meibauer, researchers at the Center for Security Studies at the Swiss Federal Institute of Technology in Zurich, define cyberspace as a virtual domain consisting of the interaction of physical and non-physical elements that allows its users to communicate unlimitedly with all parts of the world via the Internet. Cyberspace is flexible and unlimited, allowing anyone who can access it to gain access to an infinite amount of information and move without any borders. Cyberspace is no longer unnecessary in our current era, as it has become one of the most important tools used by countries to store and exchange information between their various entities. It also allows countries to manage their infrastructure with the utmost speed and with the least possible effort.[47] Many existing studies tend to view cyberspace as a domain through which actors seek to conduct cyber operations from which they gain a benefit at the expense of other actors.[48]

Although definitions of cyberspace vary, they all seem to agree on its practical aspect. Cyberspace consists of three main components. The first is the sum of physical factors, such as information technology infrastructure such as computers. The second component is intellectual factors, such as software and applications. The third component relates to the information stored by computers, the network of interactions, and the data transmitted across cyberspace.[49] Therefore, cyberspace has become one of the most important components of the modern state, which countries cannot do without in managing their affairs and various sectors, especially the vital ones.[50] The digital and technological advantages of cyberspace are met with significant risks and threats, as some exploit cyberspace to carry out cyberattacks for financial, military, political, and ideological motives. The most damaging of these risks is cyberwarfare.[51]

2.2 The Cyber War:

Just as defining cyberspace is a challenge, finding a clear term that defines cyber war is extremely difficult for academics and specialists in this and similar fields. It is unlike conventional war in terms of time and space, as cyber war takes the form of multiple temporal rounds with an unknown beginning and an undefined end. In terms of location, it has no geographical scope, as cyber wars take place in virtual space, the consequences of which are reflected in the geography of the targeted country. The United Nations Office on Drugs and Crime acknowledges the difficulty of finding a single, universal definition of cyber war. Therefore, it has resorted to describing cyber war as electronic actions that endanger and disrupt critical infrastructure systems, amounting to an armed attack.[52]

Former White House advisor Richard Clarke defines cyber war as "unauthorized penetrate into another nation's network or computer by, on behalf of, or in support of a government, or any other

---

[47] Michiel Foulon and Gustav Meibauer, "How cyberspace affects international relations: The promise of structural modifiers," *Contemporary Security Policy*, no. 3 (2024): 429.

[48] Ibid.

[49] Ibid.

[50] Ibid.

[51] ربيعي حسين وسمر محمود، "الحروب السيبرانية: المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي،" *المجلة الجزائرية للأمن الإنساني*، المجلد 7، العدد 2 (2022)، ص 175

[52] "Hacktivism, Terrorism, Espionage, Disinformation Campaigns and Warfare in Cyberspace," *United Nations Office on Drugs and Crimes*, 2019, https://shorturl.at/PTHTA.

activity that affects a computer system to add, change, or falsify data, cause a computer to crash, or damage a networked device or things controlled by the computer system.[53]" In another definition, he sees cyber war as actions taken by a nation-state to penetrate the computers or networks of another state with the aim of causing harm or disruption.[54] The difference between the two definitions is that in the first, Clarke defines cyber war as a penetration, meaning that cyber war begins with the initial attack. In the second, Clarke expands his definition to include preparations prior to the penetration. He considers the actions taken by one state to launch a cyberattack against another state to be the beginning of a cyber war, regardless of whether a penetration occurs.

Although there are many media definitions of cyber war, they cannot be taken without criticism, even though academic definitions of cyber war are still relatively few. For example, the Dutch National News Agency (NPO) defines cyber war as a war that takes place in the online world, including attacks on computers and networks for political reasons. Remote hackers can cause widespread chaos and complete disruption to a country or an entire region.[55] In this definition, we see that the Dutch National News Agency limited the causes of cyber war to political reasons only. This is not entirely true. As we will see later, there are countries that have launched cyber attacks on hostile countries for scientific reasons, with the aim of stealing modern technology that they do not possess, as Iran did when it attacked American and Western universities. In another definition, cyber war is the use of the Internet-based capabilities of a governmental or non-governmental actor to disrupt, manipulate, or destroy information contained in the computers or electronic networks that another governmental or non-governmental actor operates on.[56]

James Andrew Lewis, director of the Technology and Public Policy Program at the Center for Strategic and International Studies in Washington, defines cyber war from a US national security perspective. Lewis argues that cyber operations have created new military capabilities through the ability to remotely manipulate computers. The Internet and computer networks provide cyber tools and technologies that states use to influence, coerce, and even attack. Militaries use cyberattacks to disrupt command and control, manipulate software, and degrade weapons performance, all with the aim of achieving political or psychological impact[57].

Here, we see that Lewis confuses in his definition conventional war, in which cyber tools are used alongside conventional weapons to have an impact on the battlefield, with cyber war conducted solely behind computer screens. For example, the recent Russian war on Ukraine is a conventional war in which both sides use cyber weapons to have a psychological impact on the battlefield. In addition to the Russian-Ukrainian war, there is a covert cyber war waged by Russia against

---

[53] علاء الدين فرحات، "الحرب السيبرانية ومستقبل الأمن العالمي،" *مجلة الناقد للدراسات السياسية*، المجلد 6، العدد 2 (2022)، ص680.

[54] عمران طه عمران، "الحروب السيبرانية دراسة تأصيلية للمفهوم،" *المركز الديمقراطي العربي*، (2024/05/11)

[55] "Wat is een Cyberoorlog," *NPO*, https://shorturl.at/ghAkV.

[56] Craig B. Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?," in *Cyberspace and International Relations*, ed. Kremer, JF. and Müller, B., (Berlin: Springer, 2014), p.24.

[57] James A. Lewis, "Cyber War: Defintions, Deterrence and Foreign Policy," *Center for Strategic and International Studies (CSIS)*, (Washington, 2015), p.3.

government institutions in countries supporting Ukraine, including the Netherlands.[58] In the first case, Russia began its conventional war on Ukraine by declaring war to justify its military operations within the borders of another state. In cyber wars, which typically take place in secret, states do not need to declare war. On the contrary, states tend to deny carrying out cyberattacks to avoid incurring any legal responsibilities.

Most definitions of cyber war tend to describe operations carried out by a state with the aim of damaging another state's computers or networks, or spying on them and stealing their information. The difference in definitions of cyber war is due to the diversity of forms of cyber war and the confusion between it and other concepts such as cyberattacks, cyberterrorism, and cybersecurity. Cyber war differs from cyberattacks in that the primary actor is states, while cyberattacks can be carried out by states, groups, and individuals alike. Cyberterrorism, on the other hand, refers to all preparatory and supportive activities for terrorism that take place on or via the internet, such as recruitment, communication, and financing.[59]

2.3 Features of Cyber War:

Cyber war is an unconventional and asymmetric war, and therefore weak countries can also invest in it as a means of compensating for their weakness in conventional war.[60] conventional wars require armies, which usually consist of three main forces: land forces, air forces, and naval forces. As for cyber wars, battles take place in cyberspace and between opponents, most of whom are anonymous.[61] This makes cyber wars asymmetric war. The cost of waging a cyber war is very low compared to conventional war, and no country will face significant costs for launching cyber-attacks. Countries do not need to manufacture expensive weapons, such as advanced aircraft and fighter jets, to pose a real threat to another country. In cyberspace, warring countries are not necessarily on equal footing economically and militarily. Indeed, weaker countries militarily may outperform stronger countries in cyberspace[62] in terms of the intensity of attacks, as Iran does, for example. However, in terms of performance and effectiveness, carrying out effective attacks can cost a lot of money and preparation, as in the case of the Stuxnet virus attack on the Natanz nuclear reactor, which cost over a billion dollars at the time.

These wars also lack the deterrence model commonly found in conventional war. Deterrence in conventional war is based on punishment and retaliation against the attacker, for example, when the attacked party identifies missile launch sites or attacks launched by the attacker . In conventional war, the attacked party seeks to destroy the missile launch sites as a form of punishment or deterrence. In cyber war, however, it is difficult to identify the launch sites of attacks, and even if it is possible, it can take months or years in some cases, which negates the

---

[58] "AIVD: Russische aanvallen en spionage grenzen aan staatsterreur," *NOS*, April 24, 2025, https://nos.nl/artikel/2564804-aivd-russische-aanvallen-en-spionage-grenzen-aan-staatsterreur.

[59] Dennis Broeders, Fabio Cristiano and Daan Weggemans, "Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy," *Institute of Security and Global Affairs*, (The Hague: Leiden University, 2021), p.2.

[60] Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?, 22.

[61] فرحات، "الحرب السيبرانية ومستقبل الأمن العالمي،"، 680.

[62] Julian Richards*, Cyber-War: The Anatomy of the Global Security Threat*, (London: Palgrave Pivot, 2014), 15.

effect of deterrence through retaliation.[63] As it is impossible to identify the attacker with certainty, some countries may resort to targeting the country they believe is the attacking party in order to confirm their ability to penetrate it and the possibility of harming it.[64] Thus, in cyber war, the attacker has a clear advantage over the defender. These wars are characterized by speed, evasion, and flexibility, which give the attacker an advantage over the defending party. The absence of clear provisions and penalties in international law to counter cross-border cyber-attacks also makes them more attractive to some countries.

Cyber war is characterized, from a strategic perspective, by the absence of the traditional hierarchical chain of command, as it does not rely on the conventional form of military command or government administration. It is difficult to distinguish between military action and political action, and there are no clear, demarcating lines between civilian and military personnel.[65] In terms of danger, cyber wars differ from nuclear wars, which could directly kill millions. However, cyber wars are no less dangerous than nuclear wars. Large-scale cyberattacks can cause significant disruption within society. In other words, we are no longer merely dealing with weapons of mass destruction, but with weapons of mass disruption.[66] Another advantage of cyber war is that the risks extend beyond military sites. Cyber-attacks are not limited to military sites and their supply lines, but extend to include all of a country's infrastructure connected to the internet and computers.

2.4 The Most Prominent Forms of Weapons Used in Cyber Wars:

It is impossible to encompass all the weapons and tools used in cyber war in a single study, or even a book, because many of the weapons that have been used or are still being used have not yet been discovered. Furthermore, states are able to quickly develop new cyber weapons or update versions of previously used viruses, giving them new names and functions. Therefore, I have included the most well-known cyber weapons that have been discovered, particularly those relevant to the research objective, such as the Stuxnet virus, which was developed by Israeli and American intelligence and implanted in an Iranian nuclear reactor with the help of Dutch intelligence.

2.4.1 Logic Bombs:

Logic bombs are a type of cyberattack that secretly inserts a set of instructions into a computer system or application to cause damage. Their name derives from the fact that logic bombs only "explode" when certain conditions are met. Once activated, the malware carried by logic bombs can cause a range of harmful consequences, ranging from relatively minor consequences such as computer slowdowns or inaccessible and corrupted files to massive data loss or system crashes. Logic bombs have the potential to completely disrupt an organization's IT infrastructure.[67]

Logic bombs are typically designed and placed within a device, system, or application during its development phase. This means that the consumer purchases the device, system, or application,

---

[63] فيصل محمد عبدالغفار، *الحروب الإلكترونية*، ط1، (عمان: الجنادرية للنشر والتوزيع، 2016)، ص11-12.

[64] ناجي الشاذلي، "الجوانب القانونية للحرب السيبرانية"، *مجلة روح القوانين*، العدد 103، (جامعة طنطا 2023)، ص 4.

[65] حسين ومحمود، "الحروب السيبرانية: المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي، 178.

[66] Greathouse, “Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?, 23.

[67] Olga Knezevic, “Logic bomb definition, examples, and protection,” *Norton*, August 9, 2024, https://us.norton.com/blog/malware/logic-bomb.

which has been infected with the cyber weapon from the outset. Logic bombs are programmed to trigger when a specific event occurs or under certain conditions, enabling the attacker to take complete control of the device.[68] Logic bombs can also be used through applications downloaded on Android devices.[69] Logic bombs can be used against individuals, companies, and governments alike. The danger of logic bombs lies in the element of surprise and the significant damage they cause once activated. Detecting the attackers also poses a significant challenge, as there is a significant time lag between the preparation and activation phases, allowing the attackers enough time to cover their tracks.[70]

2.4.2 Stuxnet

Stuxnet is a highly sophisticated computer worm that exploits previously unknown vulnerabilities in Windows to infect targeted systems and spread to other systems. Stuxnet primarily targeted centrifuges at Iranian uranium enrichment facilities, with the goal of secretly disrupting Iran's nascent nuclear program. However, Stuxnet was modified over time to enable it to target other infrastructure such as gas pipelines, power plants, and water treatment plants.[71]

Stuxnet was discovered on an Iranian computer in 2010, but its development is believed to have begun in 2005. The malware surprised computer experts due to its complexity. Stuxnet was developed by US intelligence in collaboration with its Israeli counterpart to sabotage centrifuges at Iran's nuclear energy facilities at Natanz, thereby halting or delaying Iran's nuclear program.[72] Stuxnet then attacked industrial control systems used to manage vital and important facilities, such as power plants, nuclear facilities, and others. Its threat was highlighted by its ability to reprogram programmable logic controllers (PLCs), give them new commands, hide the changes it made, and display the old information it had recorded on screens, making it appear to observers that everything was proceeding normally.[73] Stuxnet reportedly destroyed about a fifth of Iran's nuclear centrifuges, infected more than 200,000 computers, and caused the performance of 1,000 to degrade.[74]

2.4.3 Duqu:

It is a preparatory weapon that carries out reconnaissance, espionage, and planting information in enemy systems, facilitating penetration, theft, sabotage, and destruction. This virus was discovered in 2011 in eight countries simultaneously: India, Iran, Vietnam, Sudan, Ukraine, the Netherlands, France, and Sweden. It was developed using an unknown programming language, the exact language of which has not been identified, and its design is based on the digital code of the Stuxnet virus. It is therefore believed to be related to the Iranian nuclear program or designed to

---

[68] إيهاب خليفة، *مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن القومي*، ط1، (القاهرة: العربي للنشر والتوزيع، 2019)، ص117.

[69] Fausto Fasano, Michele Guerra, Roberto Milanese and Rocco Oliveto, “A Dynamic Approach to Defuse Logic Bombs in Android Applications,” in *Data and Applications Security and Privacy*, ed. Gerhard Goos and Juris Hartmanis (Berlin: Springer, 2023), 358.

[70] Knezevic, “Logic bomb definition, examples, and protection.”

[71] “Stuxnet explained: What it is, who created it and how it works,” Kaspersky,” https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet.

[72] Marie Baezner and Patrice Robin, "Hotspot Analysis: Stuxnet", *Center for Security Studies (CSS*), (Switzerland, 2017), p.4.

[73] خليفة، *مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن*، 120.

[74] Stuxnet explained: What it is, who created it and how it works.”

spy on the Iranian nuclear industry. The primary function of this virus is to spy on industrial control systems and gather strategic and intelligence information about the targeted country's industries and infrastructure. This virus also has dangerous sub-functions, including enabling attackers to exploit vulnerabilities in targeted systems, destroy data on devices, or sabotage the operational devices themselves.[75]

2.4.4 Flame:

This virus was discovered in 2012 by the Iranian Emergency Response Team, where it was found on more than 1,000 devices within Iranian government and educational institutions. It was later found in several Middle Eastern countries, including Egypt, Jordan, and Saudi Arabia. Kaspersky, a cybersecurity company, believes that this virus is a cyber weapon, and that a state is behind it, not the work of independent hackers. It is a highly sophisticated virus, and its goal is not financial gain or sabotage, but rather espionage and information gathering. In cooperation with the International Telecommunication Union of the United Nations, the company has monitored more than 600 targets, ranging from governments, private companies, universities, and academic institutions.[76]

Flame can record audio conversations and all activities on the infected computer, take screen captures, record meetings and chat conversations, and turn the infected device into a point of collecting information from Bluetooth-connected devices, sending this information to the attacker. This virus is characterized by its ability to erase all data that enables investigation teams to trace its source and identify the attacker.[77]

2.4.5 Shamoon:

It is a highly destructive malware that aims to erase data from infected systems and replace it with new data. This virus was first discovered following a cyberattack, believed to be Iranian, on the American Saudi company Aramco in 2012. This breach disabled more than 30,000 of the company's computers.[78] It is believed to be the second largest cyber breach in history so far, after the breach of nuclear power facilities at Iran's Natanz plant.

2.4.6 Decoy Dog:

Decoy Dog is a sophisticated malware family discovered in April 2023 that has likely been used for at least a year in cyber intelligence operations. Its attacks are carried out via so-called command and control (C2) servers, which can manipulate network communications via malware to take control of infected networks and devices. The data exchange between the C2 server and infected devices goes unnoticed. This makes these attacks extremely difficult to detect unless they are analyzed within the context of a global threat intelligence system.[79]

---

[75] خليفة، *مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن*، 121.

[76] Dave Lee, "Flame: Massive cyber-attack discovered, researchers say," *BBC*, May 28, 2012, https://www.bbc.com/news/technology-18238326.

[77] خليفة، *مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن*، 122.

[78] Jim Pidd, "Zeer destructieve malware Shamoon is het werk van Iraanse hackers," *TECHZINE*, December 20, 2018, //shorturl.at/fkQLt.

[79] "Nieuwe Russische malware richt zich op organisaties wereldwijd," *Dutch IT Channel*, April 24, 2023, https://www.dutchitchannel.nl/news/229780/nieuwe-russische-malware-richt-zich-op-organisaties-wereld.

It remains unclear who is behind the malware, but researchers at cybersecurity firm InfoBlocks believe it is being used and developed by four actors for highly targeted operations. The observed activity is concentrated in Russia and Eastern Europe and appears to be linked to Russia's invasion of Ukraine.[80]

In addition to cyber weapons developed by states, there is also malware developed by independent hackers for the purpose of financial gain, but which states also use in their cyber wars, such as ransomware, which attacked about a quarter of Dutch companies in 2022.[81]

2.5 Conclusion:

It is still extremely difficult to find a universal and comprehensive definition of cyber war. Until now, countries have defined it based on their own perspective and understanding of their own cybersecurity. Furthermore, the international organizations and media outlets often confuse the concept of cyber war with similar concepts such as cyber-attacks, cybercrime, and cyberterrorism. However, we can still distinguish between cyber wars and conventional wars due to the clarity of the latter. As for the weapons and tools used in cyber war, they cannot be exhaustively listed, as many weapons are developed in complete secrecy and are only revealed after cyber-attacks have occurred and are investigated, which takes a long time.

3- The Iranian Cyberspace:

Studying Iran's cyber capabilities is essential to examining the geopolitical implications of the Iranian-Israeli cyber war on The Netherlands. In this chapter, I examine the Iranian cyberspace. Since the late 1990s, Iran has sought to enhance and develop its defensive and offensive cyber capabilities. This is to overcome the blockade imposed by the United States and NATO, which hinders its development of military capabilities to confront its adversaries. Iran realizes that any direct attack on the interests of the United States or its allies in the region could be considered a declaration of war, exposing Iran to further sanctions, blockades, or direct military intervention. Therefore, Iran's investment in cyberspace gives it political leverage in the regional and global balance of power, given its inability to develop military industries that are comparable to those of competing countries. This enables it to indirectly harass American interests without the risk of direct confrontation with the United States. Iran's determination to develop its cyber capabilities has increased over the past two decades, following US and Israeli cyberattacks targeting its nuclear facilities aimed at halting its nuclear program. To respond to the US and Israeli attacks targeting its

[80] "Dog Hunt: Finding Decoy Dog Toolkit via Anomalous DNS Traffic,"*InfoBlocks*, April 20, 2023, https://blogs.infoblox.com/threat-intelligence/cyber-threat-advisory/dog-hunt-finding-decoy-dog-toolkit-via-anomalous-dns-traffic/.

[81] "Ransomware game," *Centrum Informatiebeveiliging en Privacybescherming*, March 31, 2025, https://www.cip-overheid.nl/producten-en-diensten/serious-games.

nuclear program and information infrastructure, Iran needs to develop its cyber capabilities to protect its interests on the one hand and confront its cyber adversaries on the other.[82]

Enhancing its offensive cyber capabilities enables Iran to steal technical and scientific information from developed countries deprived of it under Western sanctions, and to employ stolen scientific technologies to develop its own domestic technologies. Cyber capabilities also provide Iran with the opportunity to gather intelligence on its adversaries in the Middle East, to pressure them by spreading misinformation and adopting soft war without resorting to conventional military forces.[83] We must also not forget that part of Iran's investment in cyber capabilities is directed at preserving the Iranian regime and suppressing dissenting voices. To enhance its cyber capabilities, Iran has sought since the beginning of the new millennium to consolidate its security partnerships with Russia and North Korea, both of which possess advanced cyber expertise and of their hostility toward the United States. Iran also seeks to expand its technology agreements with China and Russia to enhance its offensive and defensive cyber capabilities. However, the latter two countries are still content with signing agreements with Iran that grant it limited defensive cyber capabilities, fearing that it will become a strategic competitor in the East.[84]

To launch attacks that achieve its objectives, Iran relies on Iranian governmental and quasi-governmental cyber institutions and cyber agents in the Middle East, such as the Houthi Cyber Army and Hezbollah. In this chapter, I examine Iranian domestic cyber organizations, both official and unofficial, and regional cyber agents that constitute an additional arm of Iran in the Middle East. I draw on the study of Dr. Hassan Al-Zaro, director of the Mosul Center for Strategic Studies, whose research examines Iran's cyber strategy and its implications for the Middle East. I also draw on research presented by researchers Hiba Al-Ansari and Muthanna Al-Maari for the Tikrit University Journal in Iraq, which compares Iranian and Israeli cyber institutions. I also draw on media reports by Reuters and The National Interest, government reports from the US Department of Justice, and the website of the Tel Aviv-based cybersecurity company ClearSky Security.

3.1 Iranian governmental cyber institutions:

Iran has been able to develop its defensive and offensive cyber capabilities, circumvent the restrictions imposed on its cyber capabilities by its enemies and friends, and build an advanced cyber institutional structure that owes full loyalty to the Islamic Revolutionary Guard Corps. Together, these institutions constitute Iran's cyber army, consisting of:

3.1.1 Supreme Council of Cyberspace:

The Supreme Council of Cyberspace was established in February 2012 and reports directly to the president. It is chaired by the president, who appoints its members every three years. The council

[82] حسن الرزو، "تأثير تحولات إيران إلى الشرق على استراتيجيتها السيبرانية وانعكاساتها المحتملة على المجال الجيوسياسي السيبراني في منطقة الشرق الأوسط،" *مجلة مدارات إيرانية*، (برلين، 2023)، ص 66.

[83] حسن الرزو، "تأثير تحولات إيران إلى الشرق على استراتيجيتها السيبرانية وانعكاساتها المحتملة على المجال الجيوسياسي السيبراني في منطقة الشرق الأوسط،" 70.

[84] Ibid.

consists of ten ordinary members, in addition to legal members. Its mission is to oversee the entire Iranian cyberspace and coordinate defensive and offensive cyber operations.[85]

3.1.2 National Cyberspace Center:

It was established by a decision of the Supreme Council of Cyberspace with the aim of developing Iran's cyber capabilities, reducing its dependence on other countries' internet, developing online content that supports the country's official religious ideology, and waging a cultural war online against hostile states. The center also launches awareness campaigns for citizens to encourage them to protect their personal websites, as well as the government and official websites, from cyberattacks.[86] In 2018, a report issued by the US Treasury Department accused the National Cyberspace Center of seeking to restrict Iranians' freedom on the Internet and restricting access to Western media websites to Iran.[87]

3.1.3 Center to Investigate Organized Crime (CIOC):

Also known as the Cybercrimes Bureau, it was established in 2007 by the Islamic Revolutionary Guard Corps and reports directly to it. Its mission is to ensure the security of Iranian cyberspace and protect the Iranian electronic government. The center assisted the Iranian government during the 2009 Iranian presidential election by blocking the opposition websites and identifying opposition activists.[88]

3.2 Quasi-governmental Institutions:

As for the quasi-governmental institutions and groups that work for the government without an official capacity, it is difficult to enumerate them. In 2019, Brigadier-General Gholamreza Soleimani, Commander of the Basij militia, claimed that Iran has 1,000 cyber battalions, and each battalion consists of 500 members.[89] But the most important unofficial Iranian cyber institutions are the Iranian Cyber Army, the Basij Cyber Brigades, Helix Kitten, Charming Kitten, Shamoon Group, and the Mabna Institute Group.

3.2.1 Iranian Cyber Army:

Iran's Cyber Army comprises a large group of highly skilled IT specialists capable of carrying out professional cyberattacks. While the Iranian Cyber Army is not officially affiliated with any government agency, there is evidence that it is subordinate to the Islamic Revolutionary Guard Corps (IRGC). Some IRGC officials have pointed to the activities of the Cyber Army and its connection to the IRGC. For example, in 2011, Mojtaba Zolnour, the former deputy representative of the Supreme Leader in the IRGC, stated that Iran had successfully used the "Cyber Army" to hack into enemy websites. The Iranian Cyber Army focuses its activity on hacking Western media

---

[85] Hiba Alnasiry and Muthanna Merei, "Cyberspace Institutions in the Middle East: Iran and Israel as a model,'' *Tikrit Journal for Political Science*, (Tikrit University, 2022), p.4.
[86] Ibid.
[87] "Treasury Sanctions Individuals and Entities for Human Rights Abuses and Censorship in Iran, and Support to Sanctioned Weapons Proliferators," *U.S. Department of the Treasury*, January 12, 2018, https://home.treasury.gov/news/press-releases/sm0250.
[88] "Center to Investigate Organized Crime," *United against nuclear Iran*, https://www.unitedagainstnucleariran.com/sanctioned-person/center-to-investigate-organized-crime-cioc.
[89] "Iran Commander Says He Has 144 Active Cyber-Battalions," *Iran International*, November 17, 2020, https://old.iranintl.com/en/world/iran-commander-says-he-has-144-active-cyber-battalions.

outlets, Twitter, and government websites. The attackers who breached the Dutch security network DigiNotar in 2012 are believed to be affiliated with the Iranian Cyber Army. The hackers left a Persian signature in the hacking code, similar to one found in 2011 when Iranian hackers breached the American security company Comodo. Translated from Persian, the signature means "I sacrifice my life for the Leader [Ayatollah Khamenei].[90]

3.2.2 The Basij Cyber Brigades:

It is believed that these Basij began to be active in the cyber world after the Basij military battalions intervened in Syria in 2012 to fight alongside the forces of the former regime in Syria of Bashar al-Assad against his opponents.[91] These brigades are primarily active on social media, aiming to support the Iranian regime against its opponents. The Basij brigades are composed of unprofessional members affiliated with the Islamic Revolutionary Guard Corps, and also rely on grassroots volunteers.[92]

3.2.3 Helix Kitten:

It consists of a group of professional Iranian hackers believed to work directly with Iranian intelligence and has been active since 2015. The cyberattacks associated with this group are not sophisticated, but they are highly consistent in their choice of victims, which is directly or indirectly linked to Iran's military, financial, and political interests. It began its work by targeting organizations in the Middle East, both private companies and government institutions. It then expanded its activity to the United States, Australia, and Europe, primarily targeting the energy, education, and communications sectors.[93] In 2016, it focused its activities on government institutions and airlines, particularly Middle Eastern airlines. Between 2017 and 2018, its activity expanded to include the education and information technology sectors, particularly in West Asia and North America. In 2019, it targeted the Communications and Information Technology Commission in Saudi Arabia and the Dubai Statistics Authority. This group was exposed in mid-2019 after being hacked by a Russian hacker group.[94]

3.2.4 The Charming Kitten:

An Iranian espionage and hacking group that has been active since 2014, primarily targeting human rights activists and media outlets. The Charming Kitten group employs social engineering to target its victims. The hacker impersonates a well-known researcher or journalist and invites recipients via email to organize an event or activity allegedly organized by the impersonated

---

[90] Sommaire, "Structure of Iran's Cyber Warfare,'' *Institute Francais D'analyes Strategique*, 2022, https://shorturl.at/WMGKS.

[91] Michael Rubin, "Basij Organization Enters Cyber Operations," *American Enterprice Institute*, December 01, 2014, https://www.aei.org/articles/basij-organization-enters-cyber-operations/.

[92] Alnasiry and Merei, "Cyberspace Institutions in the Middle East: Iran and Israel as a model, 4.

[93] Matthew Armelli, Stuart Caudill and others, "The Impact of Information Disclosures on APT Operation" *SIPA Capstone Project.* (Columbia: School of International and Public Affairs,2020), p.42.

[94] "APT34: The Helix Kitten Cybercriminal Group Loves to Meow Middle Eastern and International Organizations," *Cyware*, August 22, 2019, https://www.cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae.

individual. Victims are then directed to a fake website imitating Google services such as Google Drive to upload documents and files.[95]

3.2.5 Shamoon Group:

A group that developed destructive viruses, the most effective of which was the Shamoon virus, which the group used in its attacks on American Saudi company Aramco in 2012, crippling approximately 30,000 computers. The group then evolved the same virus into Shamoon 2 and Shamoon 3, targeting Saudi Arabia again in a series of attacks between 2016 and 2017.[96]

3.2.6 Mabna Institute Group:

An Iran-based hacking group linked to the Islamic Revolutionary Guard Corps hacks into universities and academic centers to steal scientific research. Between 2014 and 2017, it hacked the computers of 144 American universities and 21 Western universities. The Mabna Institute stole more than 31 terabytes of academic data and intellectual property from the universities. In addition to academic centers and universities, the group has targeted financial sectors, most recently in 2019, when it targeted a British bank.[97]

3.3 Iran's Cyber Agents:

In addition to local governmental and quasi-governmental institutions in Iran, there are numerous cyber agents in the Middle East, such as the Syrian Electronic Army, Hezbollah Cyber Factions, and the Houthi Cyber Group. There is also cooperation between Iran and Hamas, according to what Microsoft revealed.[98]

3.3.1 The Syrian Electronic Army:

The Syrian Electronic Army was created after the outbreak of the Syrian revolution against Bashar al-Assad's regime in 2011 to support regime of al-Assad against its opponents. The Syrian Electronic Army began its operations by confronting activists of the Syrian revolution and targeting opposition websites and media outlets opposed to al-Assad's regime. Since 2013, the Syrian Electronic Army has targeted Western websites. In April of that year, it hacked the Associated Press Twitter account and tweeted a false news story about a bombing at the White House that injured President Obama. This tweet led to losses in the US stock market. The group has also expanded its activities to target Harvard University, the US Marine Corps, and Human Rights Watch.[99]

---

[95] "The Kittens Are Backin Town: Charming KittenCampaignAgainst Academic Researchers," *ClearSky Security*, (Tel Aviv: 2019), p.3-4.

[96] "Saudi Arabia says cyber attack aimed to disrupt oil, gas flow," *Reuters*, December 9, 2012, https://www.reuters.com/article/business/energy/saudi-arabia-says-cyber-attack-aimed-to-disrupt-oil-gas-flow-idUSL5E8N91UE/.

[97] "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," *Office of Public Affairs U.S., Department of Justice*, (U.S: March 28, 2018).

[98] "Iran surges cyber-enabled influence operations in support of Hamas," *Microsoft*, February 26, 2024, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas.

[99] Benjamin R. Young, "Is Bashar al-Assad's Army of Hackers Gone for Good?," *The National Interest*, April 19, 2022, https://shorturl.at/Fv8up.

In 2013, former US intelligence general Michael Hayden declared that the Syrian Electronic Army was an extension of the Iranian state and one of its cyber agents in the region. This was due to the wide range of technologies and expertise used, indicating Iranian involvement in training and directing this group. In 2014, the United States dismantled this group when Germany arrested Syrian citizen and member Peter Romar and extradited him to the United States, where he was tried. Two other members of this army were subsequently placed on the FBI's most wanted list: Firas Dardar and Imad Omar Agha.[100]

3.3.2 Hezbollah Cyber Factions:

Hezbollah Cyber Factions began its cyber activities through social media, primarily to spread propaganda and ideology among Arab audiences. Hezbollah also uses modern technology for espionage and sabotage. Most of the party's sabotage operations involved hacking traditional websites. In 2015, the Israeli company Check Point Software revealed that Hezbollah Cyber Factions had significantly developed its cyber tools with support from Iran. At the time, Hezbollah Cyber Factions, in cooperation with the Iranian Cyber Army, launched the "Volatile Cedar" campaign to hack Israeli and Western software.[101]

3.3.3 Houthi Cyber Group:

It is not known exactly when this group was founded or its organizational structure. In 2024, the cybersecurity company "Lookout" published a report stating that a group of Yemeni hackers had been spying on information belonging to several armies in the Middle East since 2019, including Egypt, Saudi Arabia, the UAE, Oman, Qatar, and Turkey. The report indicates that this group is affiliated with the Iran-backed Houthi group and has managed to hack the phones of approximately 450 victims.[102]

3.4 Conclusion:

The siege imposed on Iran by sanctions, its desire to develop and protect its nuclear program, and its desire to assert its dominance and control as a regional power in the Middle East are the primary motivations for Iran to develop its cyberspace. Iran's cyberspace consists of three structures: official government institutions responsible for developing the cyberspace and for the defense and protection of Iranian cyberspace; and quasi-governmental and non-governmental institutions that carry out illegal cyberattacks to strengthen the regime's control, confront its opponents, spy on enemy countries, and steal information and modern technology. Cyber agents in the Middle East are carrying out hacks against countries hostile to Iran.

4- The Israeli Cyberspace:

Just as I examined the Iranian cyberspace in the previous chapter, in this chapter I will examine the Israeli cyberspace. Understanding the cyberspace of both countries is a key prerequisite for

[100] Ibid.

[101] Pahlavi Pierre, "Digital Hezbollah and Political Warfare in Cyberspace," *The National Interest*, October 31, 2022, https://shorturl.at/ps453.

[102] "Lookout Discovers Houthi Surveillanceware Targeting Middle Eastern Militaries," *Lookout*, July 09, 2024, https://shorturl.at/GR0R6.

answering our research question about the impact of the Iranian-Israeli cyber war on the Netherlands. In this chapter, I will rely on David Rodman's review of The book "The battle for your computer: Israel and the growth of the global cyber-security industry". I also review Majd Ziadeh and Anas Jamil Safouri's "Cybersecurity in Israeli National Security Priorities," published in late 2024 by the Center for Arab Unity Studies. Also, I see Raghad El-Bahi's study for the Egyptian Center for Thought and Strategic Studies, "Israel's Cyber Dome: Features and Motives." I will also examine reports from the Israeli Ministry of Defense and media reports from The Times of Israel, as well as the book "Cyber war" by Egyptian military sciences researcher Faisal Abdul Ghaffar. I will also use Gawdat Bahgat research on the cyber confrontation between Iran and Israel, published in 2020 in the Middle East Policy.

Israel is considered a middle-powerful country in the real world, according to international standards of strength and weakness. When it comes to cybersecurity, however, Israel is one of the most advanced and powerful countries by global standards today. Israel possesses some of the most capable cyber capabilities in the world. Israeli entrepreneurs have founded many of today's leading cybersecurity companies, such as Check Point, CyberArk, and Palo Alto Networks. Many of them are graduates of Unit 8200, Israel's most prominent cybersecurity unit and the equivalent of the US National Security Agency.[103] Israel's security doctrine is also based on the importance of technological superiority to protect state security. This approach was approved by Ben-Gurion's government in 1948[104] and has been followed by successive Israeli governments. Israel's need and motivation to possess massive and advanced cyber capabilities are highlighted for the following reasons: recurring cyber-attacks. For example, in 2023 alone, Israel was subjected to 1,480 cyber-attacks.[105] The second motive relates to confronting regional adversaries, particularly Iran, which has acquired a significant offensive and defensive cyber force, alongside the cyber power possessed by Hezbollah, the Houthi cyber group, and other Iranian cyber agents in the Middle East, whose cyber capabilities Iran itself has contributed to developing, as we mentioned in the previous chapter. The third motive lies in securing telecommunications companies, which are often used as a gateway for hacking, as they contain a vast amount of civil and government information. The fourth motive is to enhance the cyber capabilities of the private sector, given its importance to the national economy and to reassure global companies working with Tel Aviv.[106] In addition, investing in cybersecurity services has become an important financial resource for Israel. In 2023, Israel sold cybersecurity products and services worth $10 billion.[107]

---

[103] David Rodman, "Cybermania: how Israel became a global powerhouse in the domain that is revolutionizing the future of humanity," review of *The battle for your computer: Israel and the growth of the global cyber-security industry, Routledge,* by Alon Arvatz, *Taylor and Francis Group*, Jun 26, 2024.

[104] Gawdat Bahgat, "Iranian-Israeli Confrontation: The Cyber Domain," 121.

[105] مجد زيادة، أنيس جميل صفوري، "الأمن السيبراني في أولويات الأمن القومي الإسرائيلي،" *مركز دراسات الوحدة العربية*، 2024/08/14، https://shorturl.at/yO6X6.

[106] رغد البهي، "القبة السيبرانية الإسرائيلية: السمات والدوافع،" *المركز المصري للفكر والدراسات الاستراتيجية*، 2022/08/03، https://shorturl.at/vgqbN.

[107] "Israel's Cyber Defense Capabilities," *Startup Nation Central*, August 11, 2024, https://startupnationcentral.org/hub/blog/israels-cyber-defense-capabilities/.

Regarding the institutional foundation and structure of Israel's military cyber capabilities, there is a significant scarcity of information. Although Israel possesses advanced cyber capabilities, it shrouds these capabilities in mystery and secrecy regarding their structure and architecture. The Israeli Ministry of Defense publishes sometimes news reports discussing specific cyber activities and training without providing any insight into the military structure. For example, the Israeli Ministry of Defense website contains a short newsletter from 2017 about a military cyber training exercise inspired by the game Pokémon.[108] Some conclusions can also be drawn from the scant information available to security research centers, as well as from media reports and journalistic investigations available about cyber-attacks carried out by Israel against its adversaries. Among the most important Israeli cyber units are The Unit 8200, The Unit 433 (called also Lahav 433), Israel National Cyber Directorate, the Government Infrastructure for the Internet Age, the Official Authority for Information Protection, The Unified Cyber Corps and The Israeli Cyber Dome.

4.1 The Unit 8200:

This unit is considered Israel's most powerful cyber arm. It is the largest unit in the Israeli army and can be compared to the US National Security Agency.[109] The Unit 8200 is affiliated with the Military Intelligence Directorate. Little information is available about its structure, the number of its members, and the selection process. It is believed that this unit was founded in 1948 by a group of elite Israeli computer and information engineers. Its activities have since evolved to include all areas of offensive and defensive cyber operations, as well as espionage activities. It is the primary intelligence gathering unit in military intelligence, collecting and analyzing information in multiple languages to monitor hostile activities on the internet.[110] Soldiers in this unit are responsible for developing tools for gathering information and mechanisms for analyzing, processing, and sharing it with relevant officials. In times of war, the unit joins field combat headquarters to ensure the rapid flow of information necessary to aid in the implementation of military operations.[111] This unit is credited with participating in the development of the Stuxnet virus and implanting it in centrifuges at the Iranian nuclear plant at Natanz.[112] Unit 8200 received a commendation in 2013 from the Chief of Staff of the Israeli Defense Forces in recognition of its achievements.[113]

4.2 the Government Infrastructure for the Internet Age:

It was approved in 1977 as a project of the Israeli Ministry of Finance to secure and protect the use of the Internet within government institutions. This project resulted in the creation of the Israeli Government Information Protection Center.[114] The center's mission was to monitor the development of government methods worldwide, coordinate between government ministries and

---

[108] "IDF Cyber Cadets, "Catch 'Em All" in Pokemon-Inspired Training Exercise," *The Israel Defense Forces*, March 18, 2017, https://shorturl.at/U0sDi.

[109] Alnasiry and Merei, "Cyberspace Institutions in the Middle East: Iran and Israel as a model, 12.

[110] أحمد بن علي الميموني، "الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل"، *مجلة الدراسات الإيرانية*، العدد 12(الرياض،2020)، ص 73.

[111] Military Intelligence Directorate," *IDF*, December 29, 2021, https://www.idf.il/en/mini-sites/directorates/military-intelligence-directorate/military-intelligence-directorate/.

[112] دينا محمود، "قراءة في التطور التكنولوجي العسكري الإسرائيلي: استراتيجيات وآفاق،" *مركز شاف للدراسات المستقبلية وتحليل الأزمات والصراعات*، 2024/09/22.

[113] زيادة وصفوري، "الأمن السيبراني في أولويات الأمن القومي الإسرائيلي."

[114] Gawdat Bahgat, "Iranian-Israeli Confrontation: The Cyber Domain," 121.

institutions to find solutions to problems related to information protection, and conduct research on the subject[115].

4.3 Israel National Cyber Directorate:

Israel National Cyber Directorate is responsible for protecting Israel's entire national cyberspace and building and developing Israel's cyberpower. It also works at the national level to continually enhance the level of protection for institutions and citizens, prevent and confront cyberattacks, and enhance emergency response capabilities. It issues an annual assessment of the state of cybersecurity in Israel, the most important risks that the state may face, and how to respond to them.[116]

4.4 The Official Authority for Information Protection:

This Authority was established by the General Intelligence Service in 2002, with the aim of protecting Israel's important and vital computer infrastructure from the dangers of cyber threats and attacks.[117]

4.5 National Cyber Defense Authority:

National Cyber Defense Authority: was established in 2011 after Israel was subjected to numerous cyber-attacks. The purpose of establishing this body was to coordinate civil and military cyber operations and enhance defensive and offensive cyber capabilities.[118]

4.6 The Unified Cyber Corps:

It was established in 2015 by former IDF Commander Lt. Gen. Gadi Eisenkot, with the aim of unifying the army's cyber expertise under one umbrella. This came after the increase in cyber threats to the Israeli military, particularly from Iran. In an interview with The Times of Israel, the IDF commander indicated Iran's ability to launch a surprise cyber war against the IDF, and that this corps would confront such potential threats.[119] Its mission also include managing defensive and offensive cyber operations in the military cyberspace in line with national security needs.[120]

4.7 The Unit 433:

It is a unit of the Israeli police and includes various divisions, including the cybersecurity division, which specializes in espionage to support security prosecutions.[121] Yaniv Ezani, head of the technology department and deputy head of Unit 433, describes it as Israel's equivalent of the FBI. Unit 433's highly effective technological capabilities have enabled it to pursue several cybercriminals within Israel and to uncover and dismantle organized cyber gangs inside and outside

---

[115] Alnasiry and Merei, "Cyberspace Institutions in the Middle East: Iran and Israel as a model, 13.

[116] "About Israel National Cyber Directorate," *Israel National Cyber Directorate*, April 17, 2018, https://www.gov.il/en/pages/newabout.

[117] عبدالغفار، *الحروب الإلكترونية*، 172.

[118] الميموني، "الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل"، *مجلة الدراسات الإيرانية*، 73.

[119] Mitch Ginsburg, "Army to establish unified cyber corps," *The Time of Israel*, June 16, 2015, https://www.timesofisrael.com/army-to-establish-unified-cyber-corps/.

[120] الميموني، "الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل"، *مجلة الدراسات الإيرانية*، 73.

[121] زيادة وصفوري، "الأمن السيبراني في أولويات الأمن القومي الإسرائيلي."

Israel in cooperation with cyber police agencies from other countries, such as the criminal organization 420, which was using the Telegram app to traffic drugs in Israel and around the world.[122]

4.8 The Israeli Cyber Dome:

Israel is developing a cyber defense system it calls the "Cyber Dome," similar to the "Iron Dome," after Iran launched more than 800 cyber-attacks between October 2023 and May 2024, according to Aviram Atzaba, the Israeli National Cyber Directorate's head of International Cooperation.[123] The cyber dome resembles a digital shield that counters cyber-attacks using artificial intelligence and international cooperation to detect threats in real time. Artificial intelligence analyzes various data to identify potential cyber threats and the time of their occurrence. This information is shared by officials from various sectors, who have a strong understanding of cybersecurity. Once a threat is identified, the Israeli Cyber Response Team is given the order to take appropriate action. Finally, Israel seeks to expand its international cyber network by exchanging information with countries with the goal of building a regional cyber defense network.[124] By the end of 2024, the Israeli army had conducted nine joint exercises with a US Army cyber team with the aim of developing the capabilities of the Israeli Cyber Dome.[125]

4.9 Conclusion:

The Israeli cyberspace consists of official civilian and military cyber institutions, such as Unit 8200 and The Official Authority for Information Protection. It also relies on private cybersecurity companies, formed by former Unit 8200 experts, such as Check Point and CyberArk. To develop its cyberspace, Israel relies on cooperation and partnerships with allies, such as the Netherlands, with which it exchanges modern technology, and the United States, with which it conducts joint military cyber exercises. It is unclear from the available information whether Israel has unofficial hacker groups or cyber agents working for it, as its official cyber institutions handle all declared legal tasks, as well as those that have been discovered as illegal, such as the development and implantation of the Stuxnet virus in the Iranian nuclear reactor, a task undertaken by Unit 8200, an official Israeli intelligence unit.

5- The Iranian-Israeli Cyber War:

After exploring, in the previous two chapters, the cyberspace of both Israel and Iran and how each of these countries is developing its cyber capabilities , this chapter examines when and how the

---

[122] Ami Rojkes Dombe, "Lahav-433 in the Cybercrime Era," *Israel Defense*, January 26, 2020, https://www.israeldefense.co.il/en/node/41752.

[123] ToI Staff and AFP, "As Iranian hackers grow more skilled, Israel builds 'cyber dome' to protect itself," *The Time of Israel*, May 03, 2024, https://www.timesofisrael.com/as-iranian-hackers-grow-more-skilled-israel-builds-cyber-dome-to-protect-itself/.

[124] Val Dockrell, "Israel building "Cyber Dome" to counter increased Iranian cyber attacks," *National Security News*, July 10, 2024, https://nationalsecuritynews.com/2024/07/israel-building-cyber-dome-to-counter-increased-iranian-cyber-attacks/.

[125] CYBERDOME IX Exercise With U.S. Cyber Command Concludes," *The Israel Defense Forces*, December 22, 2024, https://www.idf.il/en/mini-sites/idf-press-releases-israel-at-war/december24-pr/idf-cyberdome-ix-exercise-with-u-s-cyber-command-concludes/.

cyber war between Iran and Israel began and the most prominent attacks between the two countries over the past two decades. In preparation for answering the research question about the impact of this war between the two countries on the Netherlands, which I will discuss in the next chapter. As for references, I will rely on Gawdat Bahgat research on the cyber confrontation between Iran and Israel, and a study by researchers Veronika Netolická and Mares Miroslav entitled: "Arms Race 'in Cyberspace' - A Case Study of Iran and Israel." I will also use al-Maimouni research on the active front in the cyber world between Iran and Israel, and the digital report of Center for Strategic and International Studies which count all cyberattacks over the world since 2006 and still up to date till May 2025. I will also draw on a report by Microsoft, an Al-Araby Al-Jadeed investigative report on Israeli-Iranian cyber-attacks, and news reports by Reuters, Foreign Policy and The New York Times.

Israel outperforms Iran in terms of operational efficiency in the cyber world. Israel has been able to launch cyber-attacks against Iran and its allies that had significant repercussions, such as the Stuxnet attack, which caused significant damage to Iran's nuclear program, and the 2024 Pager attack (more on that later), which killed dozens of elite Hezbollah fighters. While Iran's cyber operations against Israel have not resulted in significant damage, they outnumber Israel in terms of quantity and intensity. Iran outnumbers Israel both in terms of the number of cyber organizations, groups, and cyber agents linked to Iran, which number approximately 1,000 cyber battalions, according to a 2019 statement by Iranian Basij commander Gholamreza Soleimani, and in terms of the number of personnel employed by these battalions, which number approximately half a million (see Chapter Three).

The Iranian-Israeli cyber war is part of the Iranian-Israeli regional conflict in the Middle East. Since it is a relatively silent war, conducted in secret, little is known about it except for what leaks to the media, such as the announcement of the disruption of the websites of vital institutions targeted in one of the two countries. Or, attacks are announced for intelligence and political purposes within the framework of exchanging and responding to accusations. The cyber war between Iran and Israel is considered one of the oldest cyber conflicts in the world history. There is no precise date for the beginning of this conflict due to the secrecy and complexity of cyber war. However, a report by the American magazine "Foreign Policy" suggests that the Iranian-Israeli cyber war began in 2006, when Israel, in cooperation with the United States, began developing a cyber weapon that became known as Stuxnet. The Stuxnet attack, as previously mentioned, aimed to sabotage computers at Iran's Natanz nuclear plant, disrupting and delaying Iran's nuclear program. In 2010, the Stuxnet virus was discovered on a large scale in Iran.[126] The Stuxnet virus destroyed about a thousand enrichment units, limiting Iran's nuclear capabilities.[127] Iran had barely recovered from the effects of the Stuxnet virus when the head of the Civil Defense Organization, Gholam Jalali, announced that a new virus called "Stars" had been discovered in Iranian government agencies. Jalali did not reveal any details about the virus or the targeted facilities. However, reports indicated that the Stars virus targeted the Bushehr nuclear reactor, which was experiencing numerous

[126] Rishi Iyengar, "The Next Israel-Iran Fight Could Be in Cyberspace," *Foreigen Policy*, April 16, 2024, https://foreignpolicy.com/2024/04/16/iran-israel-conflict-missile-attack-cyberattacks-warfare/.
[127] *76*. الميموني، "الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل"،

technical problems that contributed to delaying its operation beyond what had been expected.[128] This discovery served as an additional incentive for Iran's cyber program, as Iran realized that it could not protect its nuclear program without adopting a defensive and offensive cyber strategy that would enable it to confront its enemies and adversaries.

According to Hadi Barhani, a professor of Israeli and Palestinian studies at Tehran State University, Israel launched five major cyberattacks against Iran between 2010 and 2021, the first of which was the Stuxnet attack. In 2011, Iranian government institutions were targeted with the Duqu virus, which was not announced. Then, in April 2012, the Iranian Ministry of Oil was targeted with the Flame virus, which was intended to steal and erase information. This attack led to the disruption of the ministry's servers and those of four of its affiliated companies.[129] In 2013, the Iranian Basij website was attacked, aiming to bring down the entire site. It is believed that Israel was behind the attack.[130] In 2015, Israeli hackers launched an attack using the "Duqu2" virus, targeting the computers of three European hotels where members of the delegations tasked with negotiating the Iranian nuclear issue were staying. The purpose of this attack was to gather information about the event and the participants.[131] In May 2020, Iran was subjected to an Israeli cyberattack targeting the Shahid Rajaee port overlooking the Strait of Hormuz. That same year, in June, Israel targeted Iranian nuclear facilities at the Natanz plant.[132] In October 2021, Iran was subjected to a major cyberattack targeting 4,300 gas stations across various Iranian cities, causing significant disruption to fuel distribution in Iran for several days.[133]

As for the Iranian response to Israeli cyber-attacks, it is believed that the first Iranian cyber-attack against Israeli targets dates back to 2009, when Iran launched a series of cyber-attacks targeting the Israeli banking sector in particular, these attacks coincided with the 2009 Gaza War.[134] In 2012, Iran is attributed to a cyber-attack virus that targeted 54 Israeli officials, including embassy employees. The attack was intended to steal documents and information . Iran's attacks in response to Israeli cyber-attacks are not limited to Israel alone. Rather, its attacks extend to include Israel's Western allies and all those Iran classifies as part of the Western camp. Between 2011 and 2013, a group of Iranian hackers launched a series of attacks targeting 47 American banks and financial institutions . The civil war in Syria coincided with Gulf states' efforts to normalize relations with Israel under American sponsorship. This has influenced the course of the Iranian-Israeli cyber war and is pushing towards implicating Gulf states and exposing them to Iranian cyber-attacks.[135] In August 2012, the American Saudi company Aramco was subjected to a hack that disabled approximately 30,000 computers, causing significant financial losses for the

---

[128] "Iran says it has detected second cyber attack," *Ruters*, April 25, 2011, https://www.reuters.com/article/technology/iran-says-it-has-detected-second-cyber-attack-idUSTRE73O1OL/.

[129] صابر غل عنبري، "الحرب السيبرانية معركة بالوكالة بين إيران وإسرائيل،" *العربي الجديد*، شباط 25، 2024، https://shorturl.at/8tcJF.

[130] "Significant Cyber Incidents Since 2006", *Center for Strategic and International Studies (CSIS),* Januari 2025, https://shorturl.at/qVUds.

[131] صابر غل عنبري، "الحرب السيبرانية معركة بالوكالة بين إيران وإسرائيل"

[132] الميموني، "الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل"، *77*.

[133] صابر غل عنبري، "الحرب السيبرانية معركة بالوكالة بين إيران وإسرائيل"

[134] Veronika Netolická and Mares Miroslav, "Arms Race 'in Cyberspace' - A Case Study of Iran and Israel," *Comparative strategy* 37.5 (2018), 422.

[135] Gawdat Bahgat, "Iranian-Israeli Confrontation: The Cyber Domain," 117.

company. At the time, US intelligence accused Iran of being behind this attack . In 2013, a group of Iranian hackers attacked the control system of a dam in New York City. The attackers almost succeeded in emptying the dam's water, but on the same day, the dam's control system was disconnected from electronic devices for maintenance . In April 2020, facilities belonging to the Israeli Water Authority were subjected to a similar attack, which supports the hypothesis that Iran was behind this attack . Several months before this attack, on March 16, Iranian intelligence managed to hack the phone of Israeli politician Benny Gantz, leader of the Blue and White party, who was at the time the strongest competitor to Israeli Prime Minister Benjamin Netanyahu. Following the outbreak of the war in Gaza in October 2023, the intensity of cyber-attacks between Iran and Israel increased. According to a Microsoft report, Iran has intensified its cyber operations against Israel since the start of the war between Israel and Hamas. Half of the Iranian cyber operations that Microsoft was able to monitor targeted Israeli companies.[136]

In September 2024, Israel targeted Hezbollah, one of Iran's most important arms and military agent in the Middle East, with a military intelligence operation using cyber weapons. The operation, known as "Hezbollah Pager Operation," destroyed the wireless communication devices (pagers) used by Hezbollah to communicate among its members. The operation killed at least 12 Hezbollah members and wounded approximately 3,000 others in Lebanon and Syria, most of them Hezbollah fighters. The Iranian ambassador to Lebanon, Mojtaba Amani, was also wounded in the operation.[137] The Pager Operation can be considered the inauguration of a new era in cyber war, regardless of the methods and cyber weapons used. It is the first time that human casualties have resulted from the use of cyber weapons.

In November 2024, an Iranian hacker group targeted the aerospace, defense, and aviation sectors in Israel, the United Arab Emirates, Turkey, India, and Albania. According to Israeli reports, the hackers impersonated LinkedIn recruiters and targeted their victims with malware, offering them fake, lucrative job offers for the purpose of espionage and data theft.[138]

5.1 Conclusion:

The Iranian-Israeli cyber war began in 2006 and continued until 2009, with intermittent, mutual attacks. However, since 2009, cyber-attacks between the two sides intensified, coinciding with the war on Gaza. They intensified significantly after the Syrian civil war in 2011, when Iran intervened on the side of the Bashar al-Assad regime in Syria. Regional cyber agents affiliated with Iran's allies, such as cyber groups affiliated with Hezbollah, the Houthis, and the Syrian Electronic Army, joined the cyber war against Israel. Iran also targeted countries allied with Israel, such as the United States, and countries that Iran considers part of the Western camp, such as Saudi Arabia, the United Arab Emirates, and Turkey. Therefore, the cyber war between Iran and Israel is a chapter in the ongoing war in the Middle East between a camp led by the United States, including

[136] Clint Watts, "Iran Accelerates Cyber ops Against Israel from Chaotic Start," *Microsoft*, February 06, 2024, https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/.
[137] "Hezbollah vows revenge on Israel for deadly Lebanon pager explosions," *The Guardian*, September 09, 2024, https://www.theguardian.com/world/2024/sep/18/hezbollah-pager-explosion-lebanon-israel-gold-apollo.
[138] "Significant Cyber Incidents Since 2006", *Center for Strategic and International Studies (CSIS)*.

Israel and the Arabian Gulf, (relatively Turkey) and an Iranian-Russian camp, including Baghdad, the Houthis, and Syria, before the fall of Bashar al-Assad's regime at the end of 2024.

6- The Implications of the Iranian-Israeli cyber war on the Netherlands:

In the introduction to this paper, I reviewed Dutch-Iranian-Israeli relations. Then, in the first chapter, I discussed the meaning of cyber war, how it differs from conventional war, and the most important weapons used in it. Then, in the second and third chapters, I examined the cyberspace of both Iran and Israel. Then, in the fourth chapter, I examined the Iranian-Israeli cyber war. Researching all of the above was necessary to answer the research question, as in this chapter I will examine the geopolitical implications of the Iranian-Israeli cyber war on the Netherlands. In this chapter I will rely on official Dutch government sources from the Dutch government (Rijksoverheid), Civil Intelligence Service (AIVD), Military Intelligence (MIVD), the National Coordinator terrorism and Security (NCTV) and The Dutch Ministries of Foreign Affairs and the Interior. I will also look into the Volkskrant investigation, which I mentioned earlier, and the role of Dutch intelligence in the Stuxnet operation.

As I noted earlier, Iranian cyberattacks are not limited to Israel alone, but also target countries it considers Israel's allies. Iran's foreign policy approach to the world remains based on a Cold War mentality. Iran divides the international community into two camps: a Western capitalist camp led by the United States, which supports Israel's policies in the East, including its anti-Iran policies; and a fragmented Eastern camp, whose leadership is contested by Russia and China. Iran attempts to leverage the countries of this camp to strengthen its regional position and develop its cyber tools. In contrast, Israel often launches its attacks in cooperation or in consultation with allied countries, particularly the United States. Consequently, the implications of the Iranian-Israeli cyber war extend beyond the borders of these two countries. Regarding the implications of the Iranian-Israeli cyber war on the Netherlands, this war has affected the Netherlands several times. At the beginning of its cyber war against Iran, Israel implicated the Netherlands when it used a Dutch agent to implant the Stuxnet virus at Iran's Natanz nuclear facility. In 2005, Dutch intelligence recruited a Dutch agent named Erik van Sabben to implant the Stuxnet virus inside the Natanz nuclear reactors, and he successfully completed his mission in 2007.[139] Dutch intelligence was not involved in the initial stages of the operation. The recruitment of Sabine and the planting of the virus were preceded by the preparation and development of the virus itself, which cost more than a billion dollars. This phase was the result of joint efforts between Israeli and American intelligence.[140]

According to the Volkskrant investigation, Dutch intelligence was unaware of all the details of the operation. It knew it was participating in a sabotage operation, but it was unaware of the seriousness of what its agent, Sabben, was doing. An intelligence source told the newspaper, "The

[139] Modderkolk, “Sabotage in Iran”.
[140] Ibid.

Americans exploited us... It was an act of war." The newspaper also suggests that Dutch politicians were unaware of the operation, and Dutch intelligence may have participated in the operation without consulting the government[141]. Assuming that Iranian investigations discovered early on the identity of the agent who planted the Stuxnet virus in its nuclear reactors, this means that the Iranian cyberattacks against the Dutch company DigiNotar in 2012 may have been part of a cyber deterrence operation or cyber retaliation. This operation occurred at a time when Iran was also launching cyberattacks against American banks in the United States and against American interests in the Middle East, such as the cyberattack against the American Saudi company Aramco in Saudi Arabia in 2011. Therefore, the impact of this cyberattack on the Netherlands was not limited to a geopolitical dimension, as Iran emphasized its repositioning of the Netherlands within the Western capitalist camp hostile to Iran. It also extended to the involvement of the Netherlands in the operation, with its intelligence services recruiting one of its citizens to carry out the operation.

A report of "The National Interest" indicates that Iran is modifying and developing the cyber weapons that used against it.[142] This may have been the case after Iran was attacked by Stuxnet and discovered in 2010. The following two years, 2011 and 2012, saw sophisticated Iranian cyberattacks against the United States, the Netherlands, and Israel, as well as the American-Saudi oil company Aramco, in which each of these countries has significant economic interests. If true, this would mean that the Stuxnet attacks, which were intended to undermine Iran's nuclear program, awakened Iran to the need to develop its cyber tools and technological expertise to protect its nuclear program on the one hand and to strengthen its regional and international standing on the other. Iran also seeks to obtain modern technology through cyberattacks for espionage and the penetration of universities and scientific research centers, particularly in the West. This is because, due to Western sanctions, Iran is deprived of much of the modern technology produced by Western countries. In addition, its allies in the Eastern bloc, China and Russia, are trying to grant it limited cyber capabilities to prevent it from becoming a regional competitor. Dutch educational institutions have been subjected to cyberattacks. In 2019, Maastricht University was subjected to a cyberattack, and in 2021, the University of Amsterdam was subjected to a cyberattack. In the summer of 2021, the research funding organization (NWO) was subjected to cyberattacks that resulted in the theft of personal data from 530,000 people at the Arnhem and Nijmegen universities of applied sciences.[143] The most recent of these cyberattacks was the attack on the Eindhoven University of Technology on January 11, 2025.[144]

Although there is no evidence that Iran may be behind these attacks on Dutch educational institutions, there are strong indications that Iran may be behind these operations for the following reasons: Iran has a long history of cyberattacks on Western academic institutions. Between 2013 and 2017, an Iranian group targeted more than 144 American universities and academic institutions and 176 universities in 21 other countries.[145] Iran's need for technology and the results

[141] Ibid.

[142] Pahlavi Pierre, "Digital Hezbollah and Political Warfare in Cyberspace," *The National Interest*, October 31, https://shorturl.at/ps453.

[143] "TU Eindhoven getroffen door cyberaanval," *DELTA*, 13/01/2025, https://shorturl.at/rwLWN.

[144] "Cyberaanval," *Eindhoven University of Technology*, January 12, 2025, https://www.tue.nl/nieuws/cyberaanval.

[145] الميموني، "الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل"، 77.

of Western scientific research in light of the blockade and sanctions imposed on it, especially with the intensification of the cyber war between it and Israel and Israel's technological and cyber superiority over Iran, which places the latter in a state of constant threat. Technological and cyber cooperation between Israel and the Netherlands means that access to Dutch technology is tantamount to access to technology used in Israel. A 2022 government report issued by Military Intelligence (MIVD), Civilian Intelligence (AIVD), and the National Coordinator terrorism and Security (NCTV) ranked Iran among the top countries posing a cyber threat to the Netherlands and identified the motive behind Iranian attacks as the goal of obtaining technology and scientific research results from Dutch universities.[146] The 2024 NCTV report also places Iran on the list of countries that pose a cyber threat to the Netherlands, alongside Russia and China, and adds another incentive: Iran's desire to spy on the Netherlands for geopolitical reasons.[147]

In addition, cyber-attacks and wars on the Netherlands have internal and external political implications. In terms of internal implications, the government appears to need to allocate more money from the state budget for cybersecurity.[148] This is for the purpose of ongoing scientific research to develop cybersecurity needs, on the one hand, and to expand cybersecurity awareness programs, on the other. In terms of external political implications, this is evident in the need for countries to engage in greater international cooperation to confront cyber threats. In 2023, the government approved the Cyber Cooperation Strategy for 2023-2028, after sensing the threat of a cyber war that Russia might wage against Europe in the wake of its war in Ukraine.[149] Iran is certainly cooperating with its ally, Russia, if such a war were waged against Europe. This highlights the need for greater cooperation with allied countries in the field of cybersecurity, not only at the European and NATO levels, but also globally.

In light of these international geopolitical risks and complexities, it would be good for the Netherlands to look eastward to cooperate with allied countries that are suffering from the risks and repercussions of the Iranian-Israeli cyber war, such as Saudi Arabia, which is constantly striving to develop its cyber capabilities. Two years ago, I conducted research comparing the Saudi and Dutch government information security approaches, with the aim of identifying lessons that the Netherlands could learn from the Saudi information security approach after both countries were subjected to widespread cyber-attacks, carried out by Iran, during the same period. As I mentioned earlier, DigiNotar was hacked in the summer of 2011, and Saudi Aramco was hacked several months later. My research concluded that: Saudi Arabia established a unified approach to information security for governmental institutions in 2014, after previously being left to the initiative of each institution or ministry individually.[150] However, the information security approach that was developed in 2014 was approved as a binding approach for all government institutions and was designed in a flexible manner to serve as a basic umbrella for all government institutions and leave room for each institution to develop its own approach under this umbrella in a manner

[146] "Dreigingsbeeld Statelijke Actoren 2," *AIVD, MIVD en NCTV*, (November, 2022), 4.
[147] "Cybersecuritybeeld Nederland 2024," *NCTV*, (October, 2024), 44.
[148] "Cybercrime bestrijden," *Rijksoverheid*, February 02, 2025, https://shorturl.at/2OuKA.
[149] "International Cyber Strategy 2023-2028," *Ministery of Foreign Affairs*, September 12, 2023.
[150] "Information Security Policies and Procedures Framework," *Communication and Information Technology Commission*, (Riyadh, 2014).

that is consistent with the size of the institution, the scope of its work, the diversity of its departments, the number of its employees, and the potential risks to which it may be exposed.[151] The Saudi information security approach requires governmental institutions to adopt information security as an ongoing process, rather than a project that ends with its establishment. This is in terms of business continuity. In terms of establishment and implementation, this process is subject to a project management and implementation mechanism.[152] The Saudi information security approach also focuses primarily on the human element, considering that humans are the primary drivers of technology. It recommends implementing awareness and training programs for employees based on their needs and the tasks they perform.[153] The Saudi information security approach also took into account the diversity of global sources and expertise. In addition to the global standards that must be followed, the Saudi information approach adopts the expertise of the American Federal and its German counterparts, in addition to Saudi national laws resulting from local expertise.[154] However, although the Saudi information security approach is flexible enough to accommodate all government institutions, it is noted that it is highly centralized within the institution itself, as the general manager delegates all authority to the institution, even technical authority that should be in the hands of technical managers.

The Dutch information security approach (BIO), which was approved in 2019[155] as a binding approach for all government institutions, is based on distinguishing between three levels of procedures: low, medium, and high. The institution itself is left to adopt one of these levels after conducting a comprehensive risk assessment that is repeated periodically and as needed.[156] What distinguishes BIO from Saudi one is that it is less centralized in the distribution of responsibilities and roles, which gives specialized employees more freedom and creativity in meeting their job responsibilities, which is what the world of cybersecurity needs.[157] BIO places a heavy emphasis on technology and suppliers at the expense of the human element, devoting less attention to employee awareness and training than its Saudi counterpart. Furthermore, considering the sources of expertise BIO relies on, it relies primarily on global information security standards and local expertise, paying very little attention to the expertise of other countries.

7- Conclusion:

The scope of cyber-attacks and wars between countries has expanded, especially in the last decade. In light of today's political conflicts and disputes between many countries, each country seeks to develop its cyber tools and produce more cyber weapons. This is due to the advantages of these wars, including their low production costs, the attacker's ability to conceal himself, and the absence of effective international laws to regulate the cyber world and its dynamics. This

[151] "Information Security Policies and Procedures Framework," 12.
[152] "Information Security Policies and Procedures Framework," 33-40.
[153] "Information Security Policies and Procedures Framework," 90-100.
[154] "Information Security Policies and Procedures Framework," 13.
[155] "Baseline Informatiebeveiliging Overheid (BIO)," *Digitale Overheid,* https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/bio-en-ensia/baseline-informatiebeveiliging-overheid/.
[156] "Baseline Informatiebeveiliging Overheid (BIO)," 17-18.
[157] "Baseline Informatiebeveiliging Overheid (BIO)," 14-15.

encourages warring countries today to resort to cyber wars to exert political pressure and obtain greater gains from their rivals at the lowest possible cost. With the increasing use of cyber weapons, no country in today's world can distance itself from these wars. Because the geography of countries at war cyberattacks is severely affected, despite their lack of a role on the battlefield, the effects of these wars are no longer limited to countries neighboring the warring states. They can extend to countries thousands of kilometers away, as is the case with the impact of the Israeli-Iranian cyber war on the Netherlands.

The Netherlands has extensive relations with both countries. Dutch-Israeli relations can be described as distinguished and have been ongoing since the establishment of the State of Israel. The strength of Dutch-Israeli relations stems from historical reasons, such as the aftermath of World War II and the Holocaust, which took the lives of millions of Jews in Europe. These reasons also stem from social reasons, as Dutch society supports Israel more than other Western countries such as the United States, Germany, and France. They also stem from political reasons, as Dutch governments have supported Israel politically and militarily in all its wars with the Arabs, from the 1948 war to the recent Gaza war. In addition to the distinguished Dutch-Israeli relations, the two countries are linked by economic, military, scientific, technological, and cyber cooperation. On the other side, Dutch-Iranian relations have witnessed significant ongoing tensions since the fall of the Shah, who was close to the Netherlands, but since the rise of the anti-American and anti-Western Khomeini regime in Tehran in 1979, which revoked all Dutch companies' licenses in Tehran. There were attempts to break the ice of the tense relationship between the two countries between 2015 and 2017, but they ultimately failed.

Iran and Israel are engaged in a political conflict that has escalated, particularly in recent years, alongside a silent war raging in cyberspace since at least 2006-2007. The two countries are competing to win this war by developing their cyber tools, whether through cyber cooperation with advanced countries in this field, as in the case of Iran, Russia, China, and North Korea, or in the case of Israel with Western cooperation, particularly with the United States and the Netherlands in the field of technology and cybersecurity. Israeli-American-Dutch cooperation is not limited to technical cooperation, but extends to military cyber training and intelligence activities.

Consequently, the Netherlands has been and continues to be significantly affected by the Iranian-Israeli cyber war, both directly as a result of its involvement in operations, such as the planting of the Stuxnet virus in the Iranian nuclear reactor, which placed the Netherlands at the heart of this war. This war also takes its toll on the Netherlands, as a result of Iran confirms its classification of the Netherlands as part of the Western camp supporting Israel, and hostile to Iran. This war also casts a shadow over the Netherlands due to scientific and technological cooperation with Israel and Iran's desire to obtain modern technology, which it is deprived of due to sanctions, for use in its cyber war against Israel. This leaves the Netherlands facing additional internal and external geopolitical implications. The internal implications are manifested by the government being forced to allocate more budgetary resources for cybersecurity and scientific research in this field. The external implications are reflected in the Netherlands' tendency to conclude more international agreements and join initiatives to enhance international cooperation in the field of cybersecurity.

8- Bibliography:

"About Israel National Cyber Directorate." *Israel National Cyber Directorate*. April 17, 2018. https://www.gov.il/en/pages/newabout.

"AIVD: Russische aanvallen en spionage grenzen aan staatsterreur." *NOS*. April 24, 2025. https://nos.nl/artikel/2564804-aivd-russische-aanvallen-en-spionage-grenzen-aan-staatsterreur.

"Algemeen ambtsbericht Iran van mei 2022." *Rijksoverheid*. May 31, 2022. https://www.rijksoverheid.nl/documenten/ambtsberichten/2022/05/31/algemeen-ambtsbericht-iran-van-mei-2022.

Alnasiry, Hiba and Merei, Muthanna. "Cyberspace Institutions in the Middle East: Iran and Israel as a model.'' *Tikrit Journal for Political Science*. (Tikrit University, 2022).

Ami Rojkes Dombe, "Lahav-433 in the Cybercrime Era," *Israel Defense*, January 26, 2020, https://www.israeldefense.co.il/en/node/41752.

"APT34: The Helix Kitten Cybercriminal Group Loves to Meow Middle Eastern and International Organizations." *Cyware*. August 22, 2019. https://www.cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae.

Armelli Matthew, Caudill Stuart and others. "The Impact of Information Disclosures on APT Operation." *SIPA Capstone Project.* (Columbia: School of International and Public Affairs,2020).

Bahgat, Gawdat. "Iranian-Israeli Confrontation: The Cyber Domain." *Middle East Policy, Vol. XXVII*, no. 3 (2020).

Baezner Marie and Robin Patrice. "Hotspot Analysis: Stuxnet." *Center for Security Studies (CSS)*. (Switzerland, 2017).

"Brede steun Tweede Kamer voor kabinetsstandpunt: Israël heeft recht op zelfverdediging." *NOS*. October 10, 2023. https://nos.nl/collectie/13959/artikel/2493597-brede-steun-tweede-kamer-voor-kabinetsstandpunt-israel-heeft-recht-op-zelfverdediging.

Broeders Dennis, Cristiano Fabio and Weggemans Daan. "Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy." *Institute of Security and Global Affairs*, (The Hague: Leiden University, 2021).

"Celebrations for Iran and their Prosperity with The Netherlands." *Diplomat Affairs Magazine*. 2017. https://www.diplomataffairs.nl/celebrations-for-iran-and-their-prosperity-with-the-netherlands/.

"Center to Investigate Organized Crime." *United against nuclear Iran*. https://www.unitedagainstnucleariran.com/sanctioned-person/center-to-investigate-organized-crime-cioc.

"Cyberaanval." *Eindhoven University of Technology*. January 12, 2025. https://www.tue.nl/nieuws/cyberaanval.

"Cybercrime bestrijden," *Rijksoverheid*, February 02, 2025, https://shorturl.at/2OuKA.

"CYBERDOME IX Exercise With U.S. Cyber Command Concludes." *The Israel Defense Forces*. December 22, 2024. https://www.idf.il/en/mini-sites/idf-press-releases-israel-at-war/december24-pr/idf-cyberdome-ix-exercise-with-u-s-cyber-command-concludes/.

"Cybersecuritybeeld Nederland 2024." *NCTV*. (October, 2024).

Dassa Dalia, Alireza Kaye, Nader and Roshan Parisa. "A Brief History of Israeli-Iranian Cooperation and Confrontation." in *Israel and Iran: A Dangerous Rivalry.* RAND Corporation, 2011.

“Defence department, The Netherlands and Israel.” *Rijksoverheid*. https://www.netherlandsandyou.nl/web/israel/about-us/who-we-are/defence-department.

“Dreigingsbeeld Statelijke Actoren 2.” *AIVD, MIVD and NCTV*. November 28, 2022. https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2.
Dockrell, Val. "Israel building “Cyber Dome” to counter increased Iranian cyber attacks.” *National Security News*. July 10, 2024. https://nationalsecuritynews.com/2024/07/israel-building-cyber-dome-to-counter-increased-iranian-cyber-attacks/.

“Dog Hunt: Finding Decoy Dog Toolkit via Anomalous DNS Traffic.”*InfoBlocks*. April 20, 2023. https://blogs.infoblox.com/threat-intelligence/cyber-threat-advisory/dog-hunt-finding-decoy-dog-toolkit-via-anomalous-dns-traffic/.

Fasano Fausto, Guerra Michele, Milanese Roberto and Oliveto Rocco. “A Dynamic Approach to Defuse Logic Bombs in Android Applications.” in *Data and Applications Security and Privacy,* edited by Gerhard Goos and Juris Hartmanis (Berlin: Springer, 2023).

Foulon Michiel and Meibauer Gustav. “How cyberspace affects international relations: The promise of structural modifiers.” *Contemporary Security Policy*, no. 3 (2024).

Ginsburg, Mitch. “Army to establish unified cyber corps.” *The Time of Israel*. June 16, 2015. https://www.timesofisrael.com/army-to-establish-unified-cyber-corps/.

Greathouse, Craig B. “Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?.” In *Cyberspace and International Relations*, ed. Kremer, JF. and Müller, B. (Berlin: Springer, 2014).

Grünfeld, Frederik. *Nederland en het Nabije Oosten. De Nederlandse rol in de internationale politiek ten aanzien van het Arabisch-Israelisch conflict 1973-1982.* Deventer: Kluwer, 1991.

“Hacktivism, Terrorism, Espionage, Disinformation Campaigns and Warfare in Cyberspace.” *United Nations Office on Drugs and Crimes*. 2019. https://shorturl.at/PTHTA.

“Het cybersecurity woordenboek.” *Cyberveilig Nederland*. November 01, 2024. https://shorturl.at/P5jXE.

“Hezbollah vows revenge on Israel for deadly Lebanon pager explosions.” *The Guardian*. September 09, 2024. https://www.theguardian.com/world/2024/sep/18/hezbollah-pager-explosion-lebanon-israel-gold-apollo.

Huib Modderkolk. “Sabotage in Iran.” *De Volkskrant*. January 08, 2024. https://www.volkskrant.nl/kijkverder/v/2024/sabotage-in-iran-een-missie-in-duisternis~v989743/.

“IDF Cyber Cadets. “Catch ‘Em All” in Pokemon-Inspired Training Exercise.” *The Israel Defense Forces*. March 18, 2017. https://shorturl.at/U0sDi.

“Information Security Policies and Procedures Framework.” *Communication and Information Technology Commission*. (Riyadh, 2014).

“International Cyber Strategy 2023-2028,” *Ministery of Foreign Affairs*, September 12, 2023.

“Iran Commander Says He Has 144 Active Cyber-Battalions.” *Iran International*. November 17, 2020. https://old.iranintl.com/en/world/iran-commander-says-he-has-144-active-cyber-battalions.

“Iran: relatie met Nederland herstellen.” *RTL*. September 20, 2015. https://www.rtl.nl/buitenland/artikel/863021/iran-relatie-met-nederland-herstellen.

“Iran roept Nederlandse ambassadeur op het matje na AIVD-rapport over liquidatiepogingen.” *NOS*. April 24, 2025. https://nos.nl/artikel/2564953-iran-roept-nederlandse-ambassadeur-op-het-matje-na-aivd-rapport-over-liquidatiepogingen.

“Iran says it has detected second cyber attack.” *Ruters*, April 25, 2011. https://www.reuters.com/article/technology/iran-says-it-has-detected-second-cyber-attack-idUSTRE73O1OL/.

“Iran surges cyber-enabled influence operations in support of Hamas.” *Microsoft*. February 26, 2024. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas.

“Israel’s Cyber Defense Capabilities.” *Startup Nation Central*. August 11, 2024. https://startupnationcentral.org/hub/blog/israels-cyber-defense-capabilities/.

Iyengar, Rishi. "The Next Israel-Iran Fight Could Be in Cyberspace.” *Foreigen Policy*. April 16, 2024. https://foreignpolicy.com/2024/04/16/iran-israel-conflict-missile-attack-cyberattacks-warfare/.

Knezevic, Olga. “Logic bomb definition, examples, and protection.” *Norton*, August 9, 2024. https://us.norton.com/blog/malware/logic-bomb.

Koppel, van den Maartje and Kanne, Peter. *Opinieonderzoek Israël-Palestina*. (Ipsos I&O, 2024). https://www.ipsos-publiek.nl/wp-content/uploads/2024/10/opinieonderzoek-israel-palestina-definitief.pdf.

Koster, Marjolein. “Waarom is de relatie tussen Iran en het Westen zo moeizaam?.” *NPO Kennis*. August 20, 2024. https://npokennis.nl/longread/7780/waarom-is-de-relatie-tussen-iran-en-het-westen-zo-moeizaam.

Lee, Dave. “Flame: Massive cyber-attack discovered, researchers say.” *BBC*. May 28, 2012. https://www.bbc.com/news/technology-18238326.

“Levering F-35 onderdelen aan Israël in strijd met Gemeenschappelijk Standpunt EU en Wapenhandelsverdrag?.” *Gerechtshof Den Haag*. December 12, 2024. https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHDHA:2024:191.

Lewis, James A., “Cyber War: Defintions, Deterrence and Foreign Policy.*” Center for Strategic and International Studies (CSIS)*, (Washington, 2015).

“Lookout Discovers Houthi Surveillanceware Targeting Middle Eastern Militaries.” *Lookout*. July 09, 2024. https://shorturl.at/GR0R6.

Maher, Nora. “Balancing deterrence: Iran-Israel relations in a turbulent Middle East.” *Emerald Publishing Limited* 8, no. 3 (2023): 227.

Malcontent, Peter. “The Netherlands, the EU and the Israeli-Palestinian Conflict”, *European Review of International Studies*, no. 9 (2022).

“Military Intelligence Directorate.” *IDF*. December 29, 2021. https://www.idf.il/en/mini-sites/directorates/military-intelligence-directorate/military-intelligence-directorate/.

National Cybersecurity Authority. “Cyber Industry Development”. https://nca.gov.sa/ar/.

Netolická, Veronika, and Miroslav Mares. “Arms Race ‘in Cyberspace’ - A Case Study of Iran and Israel.” *Comparative strategy* 37.5 (2018).

“Nieuwe Russische malware richt zich op organisaties wereldwijd.” *Dutch IT Channel*. April 24, 2023. https://www.dutchitchannel.nl/news/229780/nieuwe-russische-malware-richt-zich-op-organisaties-wereld.

“Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps.” *Office of Public Affairs U.S., Department of Justice*. (U.S: March 28, 2018).

Pahlavi Pierre. “Digital Hezbollah and Political Warfare in Cyberspace.” *The National Interest*, October 31, 2022. https://shorturl.at/ps453.

Peeter Lorents and Rain Ottis. “Cyberspace: Definition and Implications.” *CCDCOE*. https://shorturl.at/jofZd.

Perlroth, Nicole. “In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back.” *The New York Times*. October 23, 2012. https://shorturl.at/ThJTB.

Pidd, Jim. “Zeer destructieve malware Shamoon is het werk van Iraanse hackers.” *TECHZINE*. December 20, 2018. //shorturl.at/fkQLt.

“Premier Rutte: Nederland staat achter Israël.” *NOS*. October 7, 2023. https://nos.nl/collectie/13959/video/2493198-premier-rutte-nederland-staat-achter-israel.

“Ransomware game.” *Centrum Informatiebeveiliging en Privacybescherming*. March 31, 2025. https://www.cip-overheid.nl/producten-en-diensten/serious-games.

Richards, Julian. *Cyber-War: The Anatomy of the Global Security Threat*. (London: Palgrave Pivot, 2014).

“Rijksdienst voor Ondernemend Nederland, Handel Nederland – Israël.” *Rijksoverheid*. October 2023. https://www.rvo.nl/onderwerpen/landen-en-gebieden/israel/handel.

Rodman, David. “Cybermania: how Israel became a global powerhouse in the domain that is revolutionizing the future of humanity.” review of *The battle for your computer: Israel and the growth of the global cyber-security industry, Routledge,* by Alon Arvatz. *Taylor and Francis Group*, Jun 26, 2024.

“Saudi Arabia says cyber attack aimed to disrupt oil, gas flow.” *Reuters*. December 9, 2012. https://www.reuters.com/article/business/energy/saudi-arabia-says-cyber-attack-aimed-to-disrupt-oil-gas-flow-idUSL5E8N91UE/.

Schie, Matthijs van. “Na de aanslag: 4 vragen over conflict Nederland-Iran.” *EW*. September 24, 2018. https://www.ewmagazine.nl/verhaal-van-de-dag/achtergrond/2018/09/na-de-aanslag-4-vragen-over-conflict-nederland-iran-645716/.

Shlaim, Avi “Israel and the Arab Coalition in 1948.” In *The War for Palestine: Rewriting the History of 1948*, edited by Avi Shlaim and Eugene L. Rogan. Cambridge University Press, 2012.

Sommaire. “Structure ofIran’s Cyber Warfare.’’ *Institute Francais D’analyes Strategique*. 2022. https://shorturl.at/WMGKS.

“Stuxnet explained: What it is, who created it and how it works.” *Kaspersky*. https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet.

Staff, ToI and AFP, “As Iranian hackers grow more skilled, Israel builds ‘cyber dome’ to protect itself,” *The Time of Israel*, May 03, 2024, https://www.timesofisrael.com/as-iranian-hackers-grow-more-skilled-israel-builds-cyber-dome-to-protect-itself/.

The Cabinet of Ministers: The Egyptian Supreme Cybersecurity Council (ESCC). “Prime Minister’s Decree No. 2259 of 2014”. https://www.escc.gov.eg/page1_1_en.html.

“The Kittens Are Backin Town: Charming KittenCampaignAgainst Academic Researchers.” *ClearSky Security*. (Tel Aviv: 2019).

“The Netherlands and Israel: a close friendship.” *Embassy of Israel The Hague*. November 01, 2024. https://new.embassies.gov.il/netherlands/en/the-embassy/bilateral-relations.

“The Netherlands and Israel,” Political department and press-related affairs, https://www.netherlandsandyou.nl/web/israel/about-us/who-we-are/political-department.

“Treasury Sanctions Individuals and Entities for Human Rights Abuses and Censorship in Iran, and Support to Sanctioned Weapons Proliferators.” *U.S. Department of the Treasury*. January 12, 2018. https://home.treasury.gov/news/press-releases/sm0250.

"TU Eindhoven getroffen door cyberaanval," *DELTA*. January 13, 2025. https://shorturl.at/rwLWN.

"Twee medewerkers Iraanse ambassade het land uitgezet." *AD*. July 06, 2018. https://www.ad.nl/binnenland/twee-medewerkers-iraanse-ambassade-het-land-uitgezet~a4b552ccf/?referrer=https%3A%2F%2Fwww.google.com%2F.

"UN E-Government Knowladgebase." *United Nations*. February 10, 2024. https://shorturl.at/CZ8zr.

"Wat is een Cyberoorlog." *NPO*. https://shorturl.at/ghAkV.

Warnaar, Maaike. *Onze vriend op de pauwentroon*. Amsterdam University Press, 2023.

Watts, Clint. "Iran Accelerates Cyber ops Against Israel from Chaotic Start,. *Microsoft*, February 06, 2024. https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/.

Young, Benjamin R. "Is Bashar al-Assad's Army of Hackers Gone for Good?." *The National Interest*, April 19, 2022. https://shorturl.at/Fv8up.

البهي، رغد. "القبة السيبرانية الإسرائيلية: السمات والدوافع." *المركز المصري للفكر والدراسات الاستراتيجية*. 2022/08/03. https://shorturl.at/vgqbN

"البيجر القاتل.. قنبلة موقوتة في الحروب السيبرانية." *الجزيرة*. 2024/09/23، https://shorturl.at/R9Kdk.

محمد عبدالغفار، فيصل. *الحروب الإلكترونية*، ط1. (عمان: الجنادرية للنشر والتوزيع، 2016).

خليفة، إيهاب. *مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن القومي*، ط1. (القاهرة: العربي للنشر والتوزيع، 2019).

المصطفى، حمزة، *المجال العام الافتراضي في الثورة السورية*، ط1. (قطر: المركز العربي للأبحاث ودراسة السياسات، 2012).

الشاذلي ناجي. "الجوانب القانونية للحرب السيبرانية". *مجلة روح القوانين*، العدد 103. (جامعة طنطا 2023).

حسين، ربيعي و محمود، سمر. "الحروب السيبرانية: المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي". *المجلة الجزائرية للأمن الإنساني*. المجلد 7. العدد 2 (2022).

الرزو، حسن. "تأثير تحولات إيران إلى الشرق على استراتيجيتها السيبرانية وانعكاساتها المحتملة على المجال الجيوسياسي السيبراني في منطقة الشرق الأوسط." *مجلة مدارات إيرانية*. (برلين، 2023).

الميموني، أحمد بن علي. "الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل". *مجلة الدراسات الإيرانية*. العدد 12 (الرياض،2020).

عبد الوهاب عاصي. "وسائل التواصل الاجتماعي في الحراك السوري المعارض 2011-2021." *مركز جسور للدراسات*، 2021.

الرزو، حسن مظفر. "الجيش السوري الإلكتروني،" *مجلة الدراسات العسكرية والاستراتيجية*، العدد 17 (برلين، 2022).

فارس، عبيدة. "الاستراتيجية الإسرائيلية في مواجهة إيران." (مركز جسور للدراسات، 2020).

فرحات، علاء الدين. "الحرب السيبرانية ومستقبل الأمن العالمي." مجلة الناقد للدراسات السياسية. المجلد 6، العدد 2 (2022).

عمران طه عمران. "الحروب السيبرانية دراسة تأصيلية للمفهوم." المركز الديمقراطي العربي. (2024/05/11). https://shorturl.at/aQxN2

زيادة مجد ، صفوري أنيس جميل. "الأمن السيبراني في أولويات الأمن القومي الإسرائيلي." *مركز دراسات الوحدة العربية*. (2024/08/14). https://shorturl.at/yO6X6

محمود، دينا. "قراءة في التطور التكنولوجي العسكري الإسرائيلي: استراتيجيات وآفاق." *مركز شاف للدراسات المستقبلية وتحليل الأزمات والصراعات*. 2024/09/22.

عنبري، صابر غل، "الحرب السيبرانية معركة بالوكالة بين إيران وإسرائيل،" العربي الجديد، شباط 25، 2024.