Jurnal Middle East and Islamic Studies

Volume 9
Number 1 *Januari-Juni 2022*

Article 6

6-11-2022

Strengthening Cybersecurity of The United Arab Emirates After The Establishment of diplomatic Relations With Israel

Afini Nurdina Utami
Universitas Indonesia, dinaafeen@gmail.com

M. Hamdan Basyar
Badan Riset dan Inovasi Nasional, m.hamdan.basyar@brin.go.id

STRENGTHENING CYBERSECURITY OF THE UNITED ARAB EMIRATES AFTER THE ESTABLISHMENT OF DIPLOMATIC RELATIONS WITH ISRAEL

Afini Nurdina Utami[1], M. Hamdan Basyar[2]
[1]Middle East and Islamic Studies Study Program, School of Strategic and Global Studies, University of Indonesia (SKSG-UI)
[2]Political Research Center, National Research, and Innovation Agency (PRP-BRIN)

Email: afini.nurdina@ui.ac.id, m.hamdan.basyar@brin.go.id

Abstrak

Uni Emirat Arab menjalin hubungan diplomatik dengan Israel pada September 2020. Keputusan ini sejalan dengan komitmen nasional Uni Emirat Arab untuk meningkatkan pengembangan potensi negara. Kedua negara sepakat untuk meningkatkan kerjasama di bidang siber dan teknologi. Ancaman regional yang hadir dari Iran menjadi salah satu faktor pendorong kerjasama kedua negara di bidang keamanan siber. Kajian ini ingin menjawab latar belakang kedua negara meningkatkan kerjasama di bidang *cybersecurity* dan bagaimana penguatan *cybersecurity* sebagai salah satu tujuan dari kerjasama pasca diresmikannya hubungan diplomatik antara kedua negara. Penelitian ini menggunakan metode kualitatif deskriptif melalui metode kajian pustaka. Hasil kajian menyimpulkan bahwa penguatan *cybersecurity* antara Uni Emirat Arab dan Israel meningkat secara signifikan setelah normalisasi dengan berbagai aktivitas dan kesepakatan seperti diselenggarakannya *Cybertech Global Dubai*, latihan bersama di bidang *cybersecurity*, dan pembangunan perusahaan *startup* UEA-Israel pertama yang mengedepankan tema *cybersecurity*.

Kata Kunci: Uni Emirat Arab, Israel, kerjasama, *cybersecurity*.

Abstract

The United Arab Emirates established diplomatic relations with Israel in September 2020. This decision is in line with the United Arab Emirates' national commitment to enhance the development of the country's potential. The two countries agreed to enhance cooperation in the fields of cyber and technology. The regional threat posed by Iran is one of the factors driving cooperation between the two countries in the field of cybersecurity. This study aims to answer the background of the two countries' increasing cooperation in the field of cybersecurity and how to strengthen cybersecurity as one of the objectives of cooperation after the inauguration of diplomatic relations between the two countries. This research uses a descriptive qualitative method through the literature review method. The study concluded that the strengthening of cybersecurity between the United Arab Emirates and Israel increased significantly after normalization with various activities and agreements such as the holding of Cyber-tech Global Dubai, joint training in the field of cybersecurity, and the construction of the first UAE-Israel startup company that puts the cybersecurity theme forward.

Keywords: United Arab Emirates, Israel, cooperation, cybersecurity.

INTRODUCTION

The Middle East is one of the most vulnerable region to cyber threats in the world. This threat can attack governments, state facilities, and companies to the wider community connected to the internet, especially in the Gulf countries. Apart from strategic initiatives to improve cyber security, countries that have abundant resources are still easy targets for cyber-attacks. The United Arab Emirates (UAE) has long made efforts to diversify its economy and develop digital technology and innovation to meet its domestic needs. The UAE also finds that cyber-attacks have increased since the onset of the Covid-19 pandemic and its decision to normalize with Israel.

The United Arab Emirates officially normalized diplomatic relations with Israel on September 15, 2020, along with Bahrain in the United States. This normalization process has been a long and gradual process, starting in 2015 when senior Israeli officials visited Abu Dhabi and Israel opened its first diplomatic office in Abu Dhabi in relation to the International Renewable Energy Agency (Cook, 2020). This step was followed by the lifting of the economic boycott of Israel through a royal decree on August 13, 2020, and the opening of the first commercial flight of Israel's El-AI aircraft to the UAE on August 31 (News, 2020). This is a historic event in the Middle East region, especially the Gulf region. So far, they have rejected the recognition and presence of Israel as a form of defending the struggle of the Palestinian people.

The UAE's decision to establish diplomatic relations with Israel drew a backlash from Iran. Tehran is worried that the normalization decision between the UAE and Israel will threaten Iran's security. The Chief of the General Staff of the Iranian Armed Forces, Major General Mohammad Baqeri, warned that "if anything happens in the Persian Gulf and the national security of the Islamic Republic of Iran is threatened -even if only slightly-, then we will blame the UAE, and will not tolerate it" (Azodi, 2020). On the other hand, Iran has always been considered a regional security threat, due to its aggressive attitude in developing nuclear.

Iran and the UAE have a hot and cold relationship. In terms of economy, the two are close friends, but in terms of security, the two have different perceptions. Since its inception, the UAE has been at loggerheads with Iran over the ownership of the islands of Abu Musa and Tunb in the Strait of Hormuz. After Britain left the Gulf in 1971, Iran occupied the

two islands belonging to the Emirate of Ras al-Khaimah. Since then, territorial disputes between the two countries have not been properly resolved (Al-Mazrouei, 2015). In addition to territorial disputes, for the UAE, the strategic threat coming from Iran has 3 important elements, namely: its support for sectarian militias, its ambition to develop missile capabilities, and the possibility of restoring its nuclear program (Al-Ketbi, 2018). The UAE decided to sign the Abraham Accord also based on concerns over Iran (Reuters, 2022).

The Abraham Accord Peace Agreement with the headlines of the peace agreement, diplomatic relations, and full normalization between the UAE and Israel became the guideline for the decisions signed by the two countries. In contrast to the agreement between Israel and Bahrain, Morocco and Sudan (which followed the steps of the UAE to normalize), the agreement between Israel and the UAE was much more detailed and planned in the text of the signed agreement. The agreement with Bahrain, Morocco and Sudan only consists of one sheet of text with the title The Abraham Accords Declaration (State Gov, 2020), while the agreement between the UAE and Israel consists of seven sheets with additional attachments for details of bilateral cooperation to be realized. This proves that the relationship between Israel and the UAE is more planned and special compared to other countries that have normalized in the near future.

In the agreement, one of the main points is to make bilateral agreements in areas of mutual interest and to unlock the great potential of each country and the region (State Gov, 2020). The UAE is actively developing potential in the field of technology. Among other things, they made a five-year plan to build a smart city and artificial intelligence (AI) named the Zayed Smart City Project and Dubai's Smart City Project. UAE technology has also begun to reach outer space. The UAE is the first Middle Eastern country to reach Mars via The Emirates Mars Mission (Murphy, 2021). In 2017, the UAE also appointed the world's first Minister of Artificial Intelligence, H.E. Omar Sultan Al-Olama who works under the Ministry of Artificial Intelligence and Digital Economy, as a form of his commitment to support knowledge, science, and research. (arabianbusiness.com, 2017)

Israel has the same commitment, which is actively developing its potential in the cyber field. Departing from government resolution no. 3611, in 2011, namely "Advancing national cyber capabilities", currently Israel has entered

the list of the top 11 cyber power countries in the world (NCPI, 2020). Israel is also known as a start-up nation with 470 companies active in cybersecurity (Tabansky, 2022).

With the high use of digital platforms and the internet in developing and achieving their country's goals, security issues cannot be separated from the bilateral relationship between the two countries. At this time, security issues are not only related to physical conflict or direct attacks between countries but are more about attacks through cyberspace. It is more vulnerable and more dangerous.

The UAE hopes that the establishment of diplomatic relations with Israel will increase cybersecurity in their country to respond to the challenges of the times. This departs from the awareness of defense and security issues that have begun to target the cyber realm as a new domain. Previously, the land, sea, air, and space domains had become fields of conflict between the interests of various countries in the world. Cyber as a domain that has developed since the 90s is a unique domain and moves so fast beyond various boundaries of space and time. Cyber is the only domain that can cover all instruments of national power, such as diplomacy, information, military, and economics (Schreier, 2015). Therefore, cyber security for a country is an important thing and cannot be ruled out.

In the relationship between Israel and the UAE, security and defense in the cyber realm are the reinforcements in diplomatic relations between the two countries. Since the normalization of relations between the UAE and Israel was announced, most international commentary has focused solely on the political and diplomatic significance of the agreement. In fact, this relationship also forms a new digital order in the Middle East, where the cooperation between Israel and the UAE will be closer to the advancement of technology development and cyber capabilities (Soliman, 2021). Both countries share the same view of Iran's presence with its aggressive stance in the region which poses a common threat in the security sector. Israel's superior capabilities in the Middle East in the cyber field and the UAE with its technological advantages have become a mutualistic relationship for the two countries. This study aims to answer the background of the two countries in increasing cooperation in the field of cybersecurity and how to strengthen cybersecurity as one of the goals of cooperation after the inauguration of diplomatic relations between the two countries.

RESEARCH METHODS

The research in this article was conducted using qualitative research methods. According to Creswell, qualitative research is mostly inductive, with the researcher generating meaning from data collected in the field (Creswell, 2003). Researchers collect data from library sources in the form of reports, journals, and trusted news. Therefore, this research is classified into the type of literature study research. In qualitative research, the process is carried out in trying to find the meaning, process, and context of the behavior or social event that is being observed (Bakry, 2016). This research is exploratory in nature and seeks to explain the 'how' and 'why' of a social phenomenon occurring in a particular context.

The theories and concepts used in analyzing the problems in this research are the concept of national interest and the theory of balance of threat.

Concept of National Interest

In international relations, there are various perspectives in viewing national interests. The realism perspective assumes that the state is an entity or actor that is the key in relations between countries. Realists agree that foreign policy is only to provide a country's national interests and goals in international politics (Manan, 2015). The interests and goals of the state can be achieved either in harmony or not, if the national interests are achieved. On the other hand, the view of liberalism sees that the national interest must focus on achieving peace and harmony between countries. National interest is considered not to lie in state security, but in economic and market stability which must also be a reference (Umar, 2014).

Not completely agreeing with the two perspectives above, the English school sees a middle way between realism and liberalism. According to Martin Wight and Hedley Bull, state attitudes and activities in international politics form an order that allows relations between countries not only to be colored by conflict but also to stable co-existential relations (Burchill, 2005: 157-158). According to the English school, national interest is defined by the state not because of its independent and isolated position but is built based on a mutual acknowledgment of the existence of other countries and concern for the impact of their actions on these other entities (Umar, 2014). The consequence of this view is that national interests are inevitably defined based on the existence of other (state) actors. When one country or countries tries to mutually recognize the existence of other countries, then the

national interest allows for a condition where the structure of society becomes more stable and solid.

Balance of Threat Theory

In the international relations literature, a threat can be defined as a situation in which an agent or group has both the ability and purpose to cause negative consequences to another agent or group (Rousseau, 2007). The Balance of Threat theory came after the balance of power theory was deemed no longer able to represent most of the events and cooperation between countries in the world. Rather than entering alliances in response to the presence of power alone, it would be more accurate to state that states will ally with or against the most threatening power (Walt, 1985). According to the balance of threat theory, countries form alliances to form a balance against threats.

In the Balance of Threat theory, the behavior of a country entering an alliance is influenced by the presence of threats they feel from other countries. This theory was proposed by Stephen M. Walt who identified four criteria that can be used by a country to evaluate threats posed by other countries, namely aggregate power, geographic proximity, offensive capabilities, and offensive intention, and offensive intentions of a country.)

In this theory, the most important basic assumption is the definition of security itself. The relationship that exists between countries defines how their respective ideas and views about security are. For example, when a country has a large amount of power without geographical proximity or aggressive intent, it will not always be seen as a significant threat (Watson, 2002).

RESULT AND DISCUSSION

The face of digital and cyber in the Middle East region

Cybersecurity challenges in the Middle East are increasing along with the development of technology and information in the area. According to a report from the Organization of Islamic Cooperation (OIC), the region's dramatic move towards digitalization is estimated to add more than $800 billion to GDP and create more than 4 million jobs, making the Gulf State a prime target for rapidly growing cyber threats (Kausch, 2017). The Gulf's high dependence on oil and gas makes this field vulnerable to cyber threats because technology is already digital. Various attacks have been felt by countries in the Middle East, such as the attack on Saudi Arabia's Aramco oil refinery, the

attack on Iran's Natanz nuclear facility, and the attack on Qatar's Al-Jazeera news agency, on 5-8 June 2021 (Leyden , 2021).

Arab countries are the target of the highest cyber threats and attacks compared to other regions. According to the Kapersky Security Network, Saudi Arabia and the United Arab Emirates are in the 17th and 18th positions of the countries facing cyberattacks in the world and are the highest in the region (Abbas, 2018). Iran, on the other hand, is identified as both the attacker and the party being attacked. Iran is the mastermind behind 19 offensive cyber operations since 2010 and Iran has also been the target of 18 operations from other countries (Kausch, 2017).

Awareness to improve cybersecurity capabilities to respond to challenges and threats brings each country in the Middle East to continue to improve its cyber capabilities. In the Global Cybersecurity Index 2020 report, the strongest countries in the region in cybersecurity are Saudi Arabia, UAE, Oman, Egypt, Qatar, Israel, Tunisia, Morocco, Iran, and Bahrain. And the weakest are Libya, Palestine, Syria, Iraq, and Yemen (ITU, 2020). It seems that countries that are more politically, economically, and security stable are better able to carry out their cybersecurity commitments. There are five main pillars in looking at the commitments of countries to cybersecurity, namely: legal action, legal measures, organizational measures, capacity-building measures, and cooperation measures. Each country has its own strengths and weaknesses in carrying out these 5 pillars, and this commitment can change in line with the times.

Cybersecurity Policy in Israel and Its Cyber Capabilities

Israel is aware of its country's structural limitations in terms of resources, territory, and weak domestic market. Therefore, since 1990 Israel has begun to focus on developing the information and technology industry in its national goals. Israel is building an innovation ecosystem by preparing human resources, attracting funding, and investing that prioritizes cybersecurity. Leaders in Israel predict security issues that arise along with the development of technology and information at that time (Noel, 2020). In 2010, the Prime Minister of Israel, Benjamin Netanyahu, appointed a special working group to ensure that Israel will become one of the best countries in the field of cybersecurity in the future (Netolicka & Mares, 2018).

The embodiment of Israeli cyber development is fully supported by the Israeli government by establishing an ecosystem that encourages the formation of digital innovation. Israel builds human resources and provides research centers, especially in universities that can be used by entrepreneurs in establishing start-ups. Cybersecurity is the sector that is most prioritized by government policy (Noel, 2020). Education funding for this research increased from $6.9 billion dollars to $11.8 billion dollars in 2019. This figure seems to have paid off with Israeli start-up revenues from total cybersecurity exports reaching $11 billion dollars in 2021 (Ben-David , 2022).

Currently, Israel is a country that has the most significant cyber capabilities in the Middle East and North Africa, even on par with other world cyber powers such as the United States, Russia, and China (Kausch, 2017). In 2020, the Harvard Kennedy School of Foreign Affairs issued the National Cyber Power Index which contains a report on countries with a cyber power index in the world. Israel in this report is ranked 11th in the world and is the most superior in the region (NCPI, 2020). This proves Israel's seriousness in realizing its national goals. However, Israel remains ostracized in the region due to its apartheid attitude towards the Palestinian people. National security and cooperation with its neighbors are still Israel's goals that they want to achieve.

International cooperation is an Israeli strategy contained in the National Cyber Security Strategy, in which Israel invites partners from all over the world to work together and share knowledge to build solutions at the global level in the field of cybersecurity (NCD, 2017). Through partnership relations, Israel seeks to assist partner countries in strengthening their national cyber security while leveraging the cyber capabilities that have been built in their country.

UAE Technology Policy and Technology Development

Since independence in December 1971, the United Arab Emirates has relied on oil to develop its country's infrastructure. The UAE's massive development helps them in establishing links with the outside world and building links with other industries, such as manufacturing and tourism. Currently, technology is one of the most prominent sectors in the UAE and its development has the full support of the government. This view was first put forward by the Prime Minister of the United Arab Emirates, His Highness Sheikh

Muhammad bin Rashid Al Maktoum, who said: “Science, technology and innovation policy are the maps for building a better future for the generations to come. We have the human resources, effective governance, and financial resources to achieve the transformation of scientific progress in the UAE” (UAEGovernment, 2015).

The UAE has several targets to be achieved through The UAE Vision 2021. Among them is the UAE as one of the top ten countries in the world in the Global Innovation Index. Therefore, the UAE issued the STI (Science, Technology, and Innovation) policy which is a strategic decision that aims to change the economic equation and divert it from dependence on limited petroleum resources (UAEGovernment, 2015). This STI policy is not only to answer national challenges, but also to capture global opportunities. There are 25 focus areas that the UAE intends to develop in this policy, including Cybersecurity and Internet of Things and Big Data. For the UAE government, focusing on science and technology research in this area is of paramount importance.

In carrying out its policies, the UAE has several main driving targets, namely through experts, investment and incentives, universities and supporting institutions, rules and intellectual property rights, partnerships, and networks (UAEGovernment, 2015). Institutions established as research forums include: The Institute Center for Microsystems (iMicro), The Institute Center for Smart and Sustainable Systems (iSmart), and the Khalifa Semiconductor Research Center (KSRC) at Khalifa University (UAE National Innovation Strategy, 2015). The image of the modern world has become a brand of the UAE, thus becoming a mecca for smart and modern cities in this century. The current achievements of the UAE depart from the initiatives of The Smart Government and Smart City. This series of innovative technology initiatives instantly secured his position in the leading technology leadership on a global level.

The UAE does not rule out cooperating with other countries to realize its interests. In the STI policy, the UAE government states that in the field of networking and collaboration, collaboration does not only occur in the academic field and the private sector within the country. Collaboration should include cooperation between institutions from other countries. Among other things, the aim is to build leading expertise in a particular unique field through collaboration.

Strategic Thinking for Cybersecurity Cooperation

The Middle East is a region that is showing rapid growth in the world in terms of internet adoption, with more than 98 percent of the population in the GCC (Gulf Cooperation Country) region being connected to the internet (The National News, 2022). This significant growth of internet users brings with it the possibility of a significantly increased threat that can extend beyond national borders. As with other conventional defense and security, one of the best ways to deal with cyber threats is to build stronger cooperation. Countries around the world are collaborating with each other to build a strong defense in cybersecurity. For example, the ASEAN region which held the ASEAN Ministerial Conference on Cybersecurity (AMCC) was seen by international experts as a good benchmark to be followed by other regions and regions (Choudury, 2021).

National interest remains the main reason for every country to engage in international relations and establish cooperation with other countries. Security is the most important factor in the national interest of a country. This study discusses security in cyberspace which in this era has become a very significant but also very vulnerable domain. International cyber security cooperation is directed to follow The UN Group of Governmental Experts (GGE) or a group of UN government experts who agreed on the norms of responsible state behavior in cyberspace by consensus in 2010, 2013, and 2015.

Regional Security Threats

The UAE and Israel share the same perception of Iran as a security threat in the region. Through the theory of balance of threat, it can be illustrated that the factor that establishes the friendship between Israel and the UAE is not because Iran has greater power (such as foreign influence, or political power due to its high population, or military capability or technological superiority). Iran's nuclear development poses a threat not only to the UAE but also to the region. If Iran has this power, coupled with its geographical proximity, offensive power, and aggressive intentions, this is what then emerges as a threat to both countries. In addition, the strengthening of cybersecurity will sooner or later be carried out by the two countries to hone and collaborate on their potential through cooperation for the interests of each country.

The Form of Cybersecurity Cooperation between the UAE and Israel

Nearly two years after the signing of the Abraham Accord, Israel and the UAE have significantly expanded their relationship by strengthening cooperation in cyberspace. Israel is the guarantor of the Emirates' cybersecurity guarantee. This is due to the potential cyber war already underway against Iran and prompts the Gulf states to lean more towards Israel in technology and cyber. The UAE and Israel find synergies in the two potentials. The forms of strengthening the UAE's cybersecurity after normalization with Israel can be seen through the following activities:

1. *Cyber-tech Global Dubai*

Dubai is the first city after Tel Aviv to host the 2021 Cyber-tech Global Conference which was attended by the Crown Prince of Dubai, Sheikh Hamdan bin Muhammad Al Maktoum (Mayangao, 2021). This international event was initiated by Israel as the first international cybersecurity event in 2014 which was held in Tel Aviv. This event is organized by Kenes Exhibition and Israel Defense Magazine which brings together experts, organizations, companies in cyber and technology to discuss developments and trends in cybersecurity (CyberTech, 2013). Dubai will first host the 8th Global Cyber-tech event on 5-7 April 2021.

The Dubai Cyber Security Strategy is one of the initiatives launched at this event that aims to integrate protection against cyber hazards and support innovation in cyberspace. One part of the event also discussed cybersecurity after Covid-19 and its impact and dedicated the results of this discussion to map cybersecurity challenges and strategies, as well as the consequences in various sectors. The event was attended by state officials, including Crown Prince of Dubai, Sheikh Hamdan Al-Maktoum; Director General of the Israel National Cyber Directorate, Yigal Unna; to the Former Director of the CIA and NATO.

In 2022, the same conference will be held again in Dubai to talk about the biggest cyber threats and opportunities of 2022 for the UAE, the region, and globally. UAE Cybersecurity Chief Mohammed Al-Kuwaiti and founder of Cyber-tech Israel will be present as speakers. However, this event has been postponed indefinitely.

2. *Cyber Security Joint Training*

Security and defense analysts have long predicted imminent cybersecurity cooperation between the UAE and Israel. Director of the Institute for Near East and Gulf Military Analysis, Riad Kahwaji stated that cyber security will be one of the

areas of cooperation between the UAE and Israel where Israel has strong strength in this field. In the future, cooperation in system integration, unmanned aircraft, and missile defense is predicted to lead to potential cooperation (Helou, 2020).

Israel has exported some $6.5 billion in 2019 in bilateral deals, one of which is cyber technology. UAE head of cybersecurity, H.E. Dr. Muhammed al-Kuwaiti met with the Director General of the Israeli National Cyber Directorate, Yigal Unna to discuss the importance of cyber collaboration between the two countries and how it will lead to shared prosperity in all key sectors (Kogosowski, UAE cyber security head calls for a joint exercise with Israel, 2021).

Dr. Al-Kuwaiti said that the two countries should prepare a strong framework and work together to build that resilience with the aim of achieving a safe and comfortable environment. Unna agreed with the existence of joint cyber exercises between the UAE and Israel and stated that cooperation without training and practice is only a theory. “With each new exercise, you will discover flaws, new ideas for how to fix them, and new ways to raise the level of cybersecurity” (Kogosowski, UAE cyber security head calls for a joint exercise with Israel, 2021).

3. *Building a Cybersecurity Startup in the UAE*

The Abraham Accords have opened a bigger deal between the two countries. In March 2022, Synaptech announced a $100 million fund for a UAE-Israeli startup in Abu Dhabi. Synaptech is an Abu Dhabi-based company backed by the Avnon Group, an Israeli company, looking to bring the spirit of Israel's "startup nation" and innovative ecosystem to life while empowering the local technology environment (UAE). The company's goal is to invest in UAE-Israeli startups developing cybersecurity, smart cities, fintech, insuretech, and public security (Hennessey, 2022). Synaptech aims to combine technology and innovation and find out how to grow an Israeli-style business in the fast-growing UAE ecosystem (Holtmeier, 2022).

Israel has been in the startup world for a long time, even being dubbed a startup nation with more startups per capita than any other country in the world. As of 2020, Israel has around 8000 startups and 356 incubators (Noel, 2020). Since deciding to focus on developing cyber, in 1990, Israel has done a lot of trial and error to get to this point. For the UAE, this collaboration in the future can strengthen cybersecurity while creating an innovative ecosystem closer to Abu Dhabi.

CONCLUSION

Diplomatic relations between the United Arab Emirates and Israel have opened many new cooperation in the fields of technology and cyber. The United Arab Emirates is known as a high-tech nation with its ambition to develop its potential in the field of technology. Israel is known as the startup nation with the main advantage of startups engaged in cybersecurity. The points of cooperation promised in the Abraham Accord deal have been quite significant since the agreement was signed. The presence of Cyber-tech Global in Dubai plans to conduct joint exercises in the field of cybersecurity and ecosystem building and innovation through the establishment of the UAE-Israeli startup, signal that the implementation of this agreement is proceeding as planned.

BIBLIOGRAPHY

Abbas, N. (2018, March 28). *Arab Countries Facing The Highest Number Of Cyber Attacks*. Retrieved from Forbes Middle East: https://www.forbesmiddleeast.com/industry/business/arab-countries-facing-the-highest-number-of-cyber-attacks

Al-Ketbi, E. (2018, May). *The Middle East's New Battle Lines*. Retrieved from European Council of Foreign Relations: https://ecfr.eu/special/battle_lines/uae

Al-Mazrouei, N. S. (2015). Disputed Islands between UAE and Iran: Abu Musa, Greater Tunb, and Lesser Tunb in the Strait of Hormuz. *Gulf Research Centre Cambridge*, 1-32.

arabianbusiness.com. (2017, October 19). *UAE appoints first Minister for Artificial Intelligence*. Retrieved from Arabian Bussiness: https://www.arabianbusiness.com/politics-economics/381648-uae-appoints-first-minister-for-artificial-intelligence

Azodi, S. (2020, August 20). *Why is Iran concerned about the peace agreement between the UAE and Israel?* Retrieved from Atlantic Council: https://www.atlanticcouncil.org/blogs/iransource/why-is-iran-concerned-about-the-peace-agreement-between-the-uae-and-israel/

Bakry, U. S. (2016). *Metode Penelitian Hubungan Internasional* . Yogyakarta: Pustaka Pelajar.

Ben-David, R. (2022, January 20). *Israeli cybersecurity firms raised record $8.8b in 2021, exports reached $11b*. Retrieved from The Times of Israel : https://www.timesofisrael.com/israel-cybersecurity-firms-raised-record-8-8b-in-2021-exports-reached-11b/

Brecher, M. (1973). Israel's Foreign Policy: Challenges of the 1970s. *International Journal*, 748-765.

Burchill, S. (2005). *The National Interest in International Relations Theory.* London: Palgrave .

Choudury, A. R. (2021, November 15). *What the world can learn from ASEAN's cyber cooperation*. Retrieved from Gov Insider: https://govinsider.asia/resilience/w

hat-the-world-can-learn-from-aseans-cyber-cooperation-amit-roy-choudhury/

Cook, S. A. (2020, August 17). *What's Behind the New Israel-UAE Peace Deal?* Retrieved from Council of Foreign Affair: https://www.cfr.org/in-brief/whats-behind-new-israel-uae-peace-deal

Creswell, J. (2003). *Research design: Qualitative, quantitative, and mixed method approaches.* London: Sage Publications, Inc.

CyberTech. (2013, November 11). *First International Cyber Security Event Coming January 2014*. Retrieved from Businesswire: https://www.businesswire.com/news/home/20131111005580/en/First-International-Cyber-Security-Event-Coming-January-2014

Helou, A. (2020, August 26). *What kind of industrial cooperation will improved Israel-UAE relations produce?* Retrieved from Defense News: https://www.defensenews.com/global/mideast-africa/2020/08/26/what-kind-of-industrial-cooperation-will-improved-israel-uae-relations-produce/

Hennessey, Z. (2022, March 24). *First Israeli-Emirati VC fund Synaptech Capital launches*. Retrieved from The Jerusalem Post: https://www.jpost.com/business-and-innovation/all-news/article-702192

Holtmeier, L. (2022, March 25). *Synaptech Capital is pairing up with ADGM to reskill UAE labour force*. Retrieved from Arabian Business: https://www.arabianbusiness.com/industries/technology/synaptech-capital-is-pairing-up-with-adgm-to-reskill-uae-labour-force

Iswara, A. J. (2021, September 14). *Riwayat Hubungan Israel-Mesir: Dulu Perang, Kini Kerja Sama Erat*. Retrieved from Kompas.com: https://www.kompas.com/global/read/2021/09/14/131334270/riwayat-hubungan-israel-mesir-dulu-perang-kini-kerja-sama-erat?page=all

ITU. (2020). *Global Cybersecurity Index 2020.* Geneva: International Telecommuncitaion Union.

Kausch, K. (2017). *Cheap Havoc; How Cyber-Geopolitics Will Destablize the Middle East.* Washington DC: The German Marshall Fund.

Kogosowski, M. (2021, May 04). *UAE cyber security head calls for joint exercise with Israel*. Retrieved from Israel Defense: https://www.israeldefense.co.il/en/node/49182

Kogosowski, M. (2021, April 5). *UAE cyber security head calls for joint exercise with Israel*. Retrieved from Israel Defense: https://www.israeldefense.co.il/en/node/49182

Leyden, J. (2021, June 10). *Al Jazeera repels cyber-attacks that sought to disrupt media network*. Retrieved from The Daily Swig, Cybersecurity News and Views: https://portswigger.net/daily-swig/al-jazeera-repels-cyber-attacks-that-sought-to-disrupt-media-network

Manan, M. (2015). Foreign Policy and National Interest:Realism and Its Critiques. *Global & Strategis*,, 175-189.

Mayangao, C. (2021, November 17). *UAE to host cybertech global conference*. Retrieved from Mid-East.Info: https://www.proquest.com/wire-feeds/uae-host-cybertech-global-conference/docview/2598245250/se-2?accountid=17242

Murphy, D. (2021, February 9). *United Arab Emirates becomes the first Arab country to reach Mars*.

Retrieved from CNBC : https://www.cnbc.com/2021/02/09/mars-probe-uae-attempts-to-become-first-arab-country-to-reach-mars-with-hope-probe.html

NCD. (2017). *Israel National Cyber Security Strategy in Brief.* Tel Aviv: National Cyber Directorate, Prime Minister's Office, State of Israel.

NCPI, T. (2020). *National Cyber Power Index 2020.* Cambridge: Belfer Center Harvard Kennedy School for Science and International Affair.

Netolicka, V., & Mares, M. (2018). Arms race "in cyberspace" – A case study of Iran. *Comparative Strategy*, 414-429.

News, A. (2020, August 29). *UAE formally lifts economic boycott of Israel*. Retrieved from Arab News: https://arab.news/vabbw

Noel, J.-C. (2020). Israel Cyberpower: The Unfinished Development of the Start-up Nation? *Etudes de l'Ifri* , 1-40.

Reuters. (2022, May 14). *UAE's newly elected ruler sees Iran, Islamists as threat to Gulf safe haven*. Retrieved from Reuters: https://www.reuters.com/world/middle-east/uae-de-facto-ruler-sees-iran-islamists-threat-ambitious-gulf-safe-haven-2022-05-13/

Rosman-Stollman, E. (2004). Balancing Acts: The Gulf States and Israel. *Middle Eastern Studies*, 185-208.

Rousseau, D. L. (2007). Identity, Power, and Threat Perception. *Journal of Conflict Resolution*, 744-771.

Schreier, F. (2015). *On Cyberwarfare.* Geneva: DCAF Horizon.

Soliman, M. (2021, May 11). *How tech is cementing the UAE-Israel alliance*. Retrieved from Middle East Institute : https://www.mei.edu/publications/how-tech-cementing-uae-israel-alliance

State Gov. (2020, September 15). *The Abraham Accords.* Retrieved from U.S. Department of State: https://www.state.gov/the-abraham-accords/

Tabansky, L. (2022, March 21). *How Israel Became a Top Cyber Power*. Retrieved from The National Interest: https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/how-israel-became-top-cyber-power

The National News. (2022, May 04). *It isn't just Israel that needs a 'cyber Iron Dome'*. Retrieved from The National News: https://www.thenationalnews.com/opinion/editorial/2022/05/04/it-isnt-just-israel-that-needs-a-cyber-iron-dome/

(2015). *UAE National Innovation Strategy.* Abu Dhabi: Prime Minister's Office - UAE Ministry of Cabinet Affairs.

UAEGovernment. (2015). *Science, Technology & Innovation Policy in the United Arab Emirates.* Abu Dhabi: UAE Government.

Umar, A. R. (2014). BOOK REVIEW: The National Interest in International Relations Theory. *Indonesian Journal of International Studies (IJIS)*, 185-190.

Walt, S. M. (1985). Alliance Formation and the Balance of World Power. *International Security*, 3-43.

Watson, M. P. (2002). *BALANCE OF POWER vs. BALANCE OF THREAT:THE CASE OF CHINA AND PAKISTAN.* Virginia: Marine Corps University.