Institute of Arab Research & Studies

The Impact of the Israeli-Iranian Cyberwar on Arab Regional Security

A Thesis Presented By

Ahmad Mohee Mohammed Ahmad Ali

In Partial Fulfillment of the Requirements for the Degree of

Master of Arab Studies – Track of Political Sciences

Advisor

Riham Bahi, PhD

Professor of International Relations – Cairo University

2023

Abstract

In this study, we aim to measure the overall impact of the Israeli-Iranian cyberwar on the Arab regional security using the regional security complex theory of Buzan, Wæver, and de Wilde. To this end, we analyzed international relations in the Arab world, including changes in patterns of amity-enmity, mutual security dependence, and distribution of powers.

This study proved that Israeli-Iranian cyberwar had a clear impact on Arab regional security. The repercussions, dangers and threats of this cyberwar have led to fundamental changes to patterns of international relations in the Arab region, including:

- Increasing mutual Cybersecurity dependence
- Changing the patterns of amity-enmity
- Changing the balance of cyber power among the countries of the region.

This finally resulted in the formation of an Arab regional Cybersecurity complex, at the initiative of the Kingdom of Saudi Arabia with participation from the Gulf Cooperation Council countries.

Keywords: *cyberwar, Arab regional security, regional cybersecurity complex, Saudi Arabia, Israel, Iran*.

Introduction

Due to its geopolitical situation, our Arab region has recently become a stage for numerous cyber-attacks by various actors, including countries and organizations. These attacks have targeted the networks of Arab facilities, capabilities, and companies, causing huge financial losses and posing a direct threat to Arab regional security **[1]**. In the absence of a clear strategy for joint Arab action in the field of Cybersecurity, efforts of international actors to exploit the Arab cyberspace to achieve their goals through cyber-attacks are increasing. Also, in the absence of cyber defense, deterrence

mechanisms and active mutual Cybersecurity dependence among Arab States, the Arab cyberspace could become a stage for one Arab state to be cyber predated, while the rest take their seats as spectators.

Research Problem

The Iranian and Israeli threats to Arab regional security in the traditional political and strategic space are well known. After the Stuxnet attack, relocating these threats to the Arab cyberspace became a reality that cannot be ignored.

One of the most prominent signs of this relocation was the cyber-attack on the Saudi Arabian oil company Aramco on August 15, 2012, which was one of the most disabling and destructive cyber-attacks against the company. The virus "Shamoon" infected about thirty thousand workstations and destroyed the company's hard drives with all the data contained **[2]**. Also the cyber-attack on the Qatari RasGas on August 27, 2012, which was considered one of the largest attacks on the private sector at the time **[3]**. Iran was pointed to as the perpetrator of the two attacks **[4]**.

Since then, both Iranian and Saudi sides have exchanged cyber-attacks and accusations, to the extent that the chief of the Iranian Civil Defense, General Gholam Reza Jalali, stated in mid-May 2016: "His country is preparing for major cyber-attacks from Saudi Arabia, and that he considers the Sunni-majority kingdom to be its main threat next year."**[5]**

This development in the direction of the attack indicates Iran's conviction that its cyber capabilities can be useful in other fronts, away from its war with Israel. Thus, it did not hesitate to employ those capabilities to attack its regional rival, Saudi Arabia. If this is the case, we should never rule out the possibility that Israel will also use its cyber capabilities to attack Arab targets if circumstances require.

Therefore, it is important for Arab decision-makers to evaluate Iranian and Israeli cyber capabilities and to identify potential threats to Arab regional security. Also consider opportunities for cooperation in defense, deterrence, and mutual security dependence among Arab States in the field of cyber security. Through studying the dimensions of the Israeli-Iranian cyberwar and analyzing their respective cyber capabilities, the Arab States can strengthen their defenses and counter potential threats.

This opens up a wide scope for studying the phenomenon of "Israeli-Iranian cyberwar" and measuring its impact on Arab regional security since 2010. Therefore, the problem of this study lies in answering the main question: "How does Israeli-Iranian cyberwar affect Arab regional security?" Several sub-questions branch out from this main question:

- What is the impact of Israeli-Iranian cyberwar on the mutual Cybersecurity dependence among Arab States?

- What is the impact of Israeli-Iranian cyberwar on patterns of amity-enmity in the Arab region?
- What is the impact of Israeli-Iranian cyberwar on the balance of power in the Arab region?

Theoretical Framework: Regional Security Complex Theory

In the book "People, States and Fear," [6] Barry Buzan defines the security complex as "a group of states whose primary security concerns are closely linked to each other, so that the national security of each state cannot be considered in isolation from the national security of other states." The term includes both the security dimension and the concept of interdependence among neighbors, whether in the form of competition or shared interests. This framework helps to build a "comprehensive multi-level approach for analyzing security problems... designed to include an intermediate level of analysis between the global system level... and the individual state level **[7]**". It also explains that each level retains its distinctive and dynamic character for separate analysis, while also examining interactions with others for a more comprehensive understanding **[8]**.

Regional security complex theory has been developed in different directions. One of the directions has been analysis of homogeneous complexes (also called sector-specific complexes as they offer analysis of isolated “sector-specific security dynamics” **[9]**, such as regional energy security complexes or water security complexes. These examples emphasize that sector-specific regional security complexes are fundamentally linked to the concept of security. Although historically, security in international relations has primarily been associated with military threats, and therefore primarily understood as military security. Under the "expanded security agenda," however, Buzan, Waever, and De Wilde analyzed security not only in the military domain but also in political, economic, environmental, and societal security sectors.**[10]**

Based on this, cyber threats can be considered part of military conflicts as a major national security issue, and the cyber sector can be considered a distinct security sector, also cyber security regional complexes (sector-specific complexes) can be formed and defined according to this approach. Such complexes may form when distinct regional security interactions are clearly visible in cyberspace. In general, their formation may not differ from other types of sector-specific complexes. They may or may not coincide with regional security complexes in physical space. With increasing reliance on information technologies, more regional cyber security complexes may form, which also have different security dynamics than physical complexes.**[11]**

Conceptual Framework: Procedural Definition of Arab Regional Security

In light of the Regional Security Complex Theory of Buzan, Weaver, and de Wilde, Arab regional security can be defined as the set of shared security interests and/or concerns among all or some of the member states of the Arab League, or among them and neighboring and/or influential powers in the region.

Therefore, the Arab League serves as the main regional security complex, from which sub-regional security complexes can branch out. These complexes aim to achieve common interests or address shared security concerns among some or all member states of the Arab League by modifying patterns of international relations among them and neighboring or influential powers in the region, especially in terms of patterns of amity-enmity, mutual security dependence, and balance of power.

Thus, the regional security complex of the Arab League can be defined as a group of some or all member states that aim to achieve common interests or address shared security concerns among themselves or with neighboring and influential regional powers by modifying patterns of international relations in the region, especially in terms of patterns amity- enmity, mutual security dependence, and balances of power.

Literature Review: Impact of Cyberwar on Regional Security

First: Impact of Cyberwar on Mutual Security Dependence

Case Study: The Indonesian-Australian Cyberwar

Cyberwar has a direct impact on mutual security dependence among states, especially those neighboring or located within the same geographical region. There is no better example of this than the case of the cyberwar between the neighboring Indonesia and Australia. In 2013, the phone of the Indonesian President Yudhoyono was tapped by Australia, which was considered a cyber-attack **[12]**. This incident had a direct impact on cyberspace and resulted in the emergence of new security threats for both sides. It quickly led to the outbreak of a cyberwar between Australia and Indonesia, which caused numerous casualties on both government and commercial targets **[13]**.

As a result, Australia began to prioritize Cybersecurity systems as a fundamental priority **[14]**. On the other hand, Indonesia saw this attention as a threat to its own Cybersecurity. This quickly led Indonesia to sign a memorandum of understanding for cooperation in the field of Cybersecurity with Australia in 2018, particularly in the area of responding to cybercrime **[15]**.

Thus, the dynamics of international relations created a relation of mutual respect and cooperation between Indonesia and Australia stemming from the cyberwar between them. Information technology development has become one of the areas of focus for both Indonesia and Australia in maintaining regional security. This development has impacted the mutual security dependence between the two sides, as it became clear that Indonesia needed Australia to develop its Cybersecurity system and continue the mutual security dependence **[16]**.

Case Study: The Russian Cyberwar on Estonia and Baltic States

Estonia gained wide notoriety for being the victim of "the first ever coordinated cyber-attack against an entire country"**[17]**. The attacks which were originating from Russia targeted public administration resources and private companies, including banks, media outlets, telecommunications companies, and resources in both Estonia and Lithuania.
Following those attacks, Baltic States paid significant attention to cyber security, particularly with regard to potential conflicts between countries in cyberspace. Estonia in particular has carried out numerous activities related to potential cyber conflicts between countries in order to improve its preparedness for cyber threats. The most prominent of these activities was the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in the capital city of Tallinn **[18]**.

Although Latvia did not face major “publicly known” incidents in the cyber space at that time, its government did not rule out the possibility of such attacks in the future **[19]**. Lithuania also dedicated significant attention to cyber threats, following in the footsteps of Estonia and Latvia **[20]**.

Given that the three Baltic States are a distinct regional complex in cyberspace, it is also important to note their mutual security dependence. They participated in founding the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn. Since 2009, they have also regularly held tripartite specialized meetings aimed at coordinating information technology security policies. These meetings culminated in signing a memorandum of understanding among the three states on November 4, 2015, for coordinating their cyber defense policies and efforts **[21]**.

Considering that Baltic States, share a heavy reliance on information technology, face similar cyber threats, as well as share similar coordinated policies towards cyber threats, it can be said that Baltic States constitute a separate regional Cybersecurity complex that can be considered a sub-region or a sub-complex of the wider regional Cybersecurity complex of the European Union. It is clear that the cyber threats imposed by Russian cyber-attacks since 2008 have had a significant impact on enhancing mutual security dependence among Estonia, Lithuania, and Latvia **[22]**.

Second: Impact of Cyberwar on Patterns of Amity-enmity

Case Study: The Indonesian-Australian Cyberwar

Returning to the case of the Indonesian-Australian cyberwar, and looking at the relation between the two countries, we find that it has witnessed dynamic fluctuations from time to time. At a certain period, the relations between the two countries seemed very friendly, cooperative and supportive. At other times, the relations became tense, suspicious and less friendly. It is not uncommon for the nature of the relations between two countries to change rapidly in a very short period of time. When Indonesia adopted a confrontational policy with the West, as happened when Indonesia opposed the British-backed union of Malaysia in 1963, relations between Indonesia and Australia began to experience tension. Tensions increased when Indonesia annexed East Timor as its 27th province in 1976. Since then and until now, the dynamics of the relations

between Indonesia and Australia have been highly volatile. Sometimes the two countries are close and very friendly, as was the case during the presidency of Suharto and Prime Minister Paul Keating in 1992-1995. And often disputes escalate quickly, as in the times of Prime Minister John Howard and President Habibie, or during the presidency of Yudhoyono and Prime Minister Tony Abbott in 2013-2014, and generally, the pattern of amity-enmity between the two countries is dominated more by enmity than amity **[23]**.

And due to the cyberwar that took place between the two sides at the end of President Yudhoyono's term in 2013-2014, Indonesia saw the prevalence of the side of amity in its relations with Australia, for several realistic reasons, most importantly:

- The significant gap in cyber capabilities in favor of Australia
- Utilizing Australian advancement in cyber security for developing Indonesian cyber capabilities
- Ensuring the neutralization of Australian cyber forces that have grown significantly
- Avoiding cyber risks when using those forces to manage the hostile relations between the two countries
- And to cooperate in responding to external cybercrimes.

This led Indonesia to sign a memorandum of understanding for cooperation in the field of Cybersecurity with Australia In 2018, especially in responding to cybercrimes **[24]**.

Since then, the amity aspect has clearly dominated over the enmity aspect in the Indonesian-Australian relations. Even Australian Prime Minister Scott Morrison announced in 2020 that the two countries enjoy a level of "trust that underpins only the truest of friendships" while Indonesian President Joko Widodo described Australia as Indonesia's “truest friend". While these statements may be exaggerated, they may pave the way for building a type of strategic partnership that will benefit both countries in the coming decades **[25]**.

Case Study: The Russian Cyberwar on Estonia and Baltic States

In the case of the Baltic States, there was a clear pattern of amity in dealing with cyber threats originating from Russia. The role of security related to these threats was highlighted in the development of the cyber security policies for the three Baltic States. The three states share a similar security vision based on addressing cyber threats emanating from Russia, particularly after the cyber-attacks on Estonia in 2007 **[26]**.

Historically, Baltic States can be categorized as part of a regional security complex centered around Russia. However, strategic and political ties, as well as historical, cultural, and economic links, do not allow Baltic States to be separated from Poland and other EU and NATO member States **[27]**.

When Buzan and Wæver referred to Baltic States as part of a "post-Soviet" regional security complex **[28]**, these countries were not yet part of NATO and the EU, and their relations with Russia were characterized by mutual "security relations." Currently, after expanding their security measures against Russian cyber threats, and after becoming a part of NATO and the EU, enmity dominates the relations between Russia and Baltic States.

Third: Impact of Cyberwar on the Balance of Power

Many studies indicate a significant change in the balances of power resulting from the redistribution of power in the Baltic region between Baltic States and Russia, both within the "post-Soviet" regional security complex and between Baltic States and the European Union. This change became evident after the Russian-Estonian cyberwar in 2007 **[29]**.

The Russian-Estonian cyberwar experience served as a "wake-up call" for NATO, and led to the launch of the NATO's targeted cyber operations **[30]**. In 2008, the first NATO policy on cyber defense was approved. In 2010, NATO adopted a new strategic concept that included, for the first time, a cyber-agenda. Since that year, the Internet has become an integral part of NATO's agenda and later a part of its core collective defense mission **[31]**.

In Edward Rhodes' study titled "The American Vision of Baltic Security Architecture: Understanding the Northern Europe Initiative" he confirmed that the integration of border regions in northwestern Russia into a variety of economic, political, social, and cultural links would inevitably reduce Moscow's power and influence, increasing the weakening of the highly tense Russian state's authority and legitimacy **[32]**.

Since their independence and increased integration into NATO and the EU, Russia has been continuously losing influence over the Baltic States. Today Estonia, Latvia, and Lithuania are undoubtedly deeply integrated into Atlantic-European structures **[33]**, politically and culturally distancing themselves from Russian influence. As a result, Russia no longer considers Baltic States as part of the post-Soviet space but as "Northern Europe"**[34]**. It is clear that this change in balances of power began before the 2007 cyber-attacks. The drift accelerated after the 2007 cyber-attacks, during the war in Georgia, and escalated again in 2014 when Russia annexed the Crimean peninsula **[35]**.

Based on their relations across the Atlantic, Baltic States have become a crucial component of Western collective defense. Therefore, cyberwar has become an essential component of the geopolitical landscape, influencing the balance of powers and shaping regional security order **[36]**.

Impact of the Israeli-Iranian Cyberwar on Arab Regional Security

Through reviewing the case studies of countries which have formed regional security complexes, several changes can be observed in foreign relations that represent a common pattern of behavior stemming from the impact of cyberwars on the regional security.
As soon as the cyberwar looms on the horizon or the risks of cyber-attacks increase in the regional environment, countries that occupy that regional environment begin to make changes in their foreign relations by adopting some or all of the following behaviors:

- They seek to enhance and develop their own cyber capabilities, especially with regard to cyber monitoring, defense, and deterrence.
- They seek to enhance cyber capabilities at the regional level, by concluding agreements, and participating in regional and international cyber efforts, activities and entities.
- They rearrange patterns of amity-enmity in their regional environment based on the level of cooperation or competition in the field of cyber defense and security, or based on the cyber risks they face.

By adopting such behaviors in their regional environment, countries modify their patterns of foreign relations resulting in an increase in mutual security dependence, changes in patterns of amity-enmity, and in the balances of powers, leading to the formation of a regional cyber security complex among them.

Considering the dangers and risks posed by the Israeli-Iranian cyberwar on Arab States, Arab States' response to those dangers and risks varied due to the differing degrees of exposure, impact, and securitization of each Arab state. As the most effective Iranian cyber-attacks targeted the Arabian Gulf region, such as the attack on Saudi Aramco in 2012 and the attack on Qatari RasGas in 2012, GCC countries were the most responsive among the Arab states to the dangers and risks posed by the Israeli-Iranian cyberwar.

In their 2018 study **[37]**, Russell Seeger and Dania Thafer argued that by analyzing multiple indicators of general cyber readiness, such as national legislation, rankings by international organizations, and inter-state cooperation, Qatar, United Arab Emirates, and Oman were the leading cyber powers in the Gulf region, while Kuwait, Bahrain, and Saudi Arabia were relatively lagging behind.

However, as Saudi Arabia was considered the most exposed Arab country to cyber-attacks and the most affected by the Israeli-Iranian cyberwar, it was the most responsive to the dangers and risks posed by that war. Therefore, this study is focusing on the case of Saudi Arabia to identify the measures it has taken in response to the cyber threats posed by the Israeli-Iranian cyberwar.

Firstly: Impact of the Israeli-Iranian Cyberwar on Mutual Security Dependence among Arab States

Enhancing and Developing Cyber Capabilities on State Level

A state's cyber capabilities depend on the extent of the development and spread of communication and information technology among its people. During the first decade of the 21st century, Arab societies suffered from significant lag in the spread of communication and information technology. This fact has been confirmed by all related international reports, where most of them indicated a low index of technology usage skills in all Arab States and the existence of a gap between Arab States and the advanced world in terms of technological skills **[38]**. This may have been the main reason behind choosing the Arab region as a battlefield for one of the biggest and most impactful cyberwars, making it a prepared arena for various cyber-attacks and cybercrimes **[39]**.

Once the Israeli-Iranian cyberwar emerged in the horizon of the Arab region with its dimensions and goals revealed, Arab States began to realize the importance of developing their own cyber capabilities, especially Saudi Arabia, as the largest Arab State subjected to cyber-attacks **[40]**. Each State has started to develop its own legislative framework, communication infrastructure, and information technology, paving the way for a tangible development in its own cyber capabilities.

As an important ally of the United States and a guardian of its strategic interests in the region, also due to the historical hostility between it and Iran; the vital national infrastructure of the Kingdom of Saudi Arabia has been targeted several times by Iran during the Israeli-Iranian cyberwar **[41]**. Since 2017, the Kingdom of Saudi Arabia has become the target of the largest number of cyber-attacks in the Middle East, nearly 60 million cyber-attacks daily targeting public and private sector aiming to destabilize the Saudi economy **[42]**.

A survey conducted by Tenable showed that 95% of Saudi companies faced cyber threats that affected their operations during 2019. The survey also revealed that 85% of Saudi participants reported a significant increase in cyber threats in 2018 and 2019, leading to data loss, ransomware payments, or financial losses **[43]**. In addition, a report by the Israeli Institute for National Security Studies concluded that Saudi Arabia is among the most targeted countries online in the world, and Iran is believed to be the main source of the attacks. For example, 42% of the cyber-attacks carried out by the Iranian APT33 group were directed against the Kingdom. The report also highlighted that Saudi Arabia remains highly vulnerable to cyber-attacks, as a recent study showed that only 4 out of 10 Saudi business leaders mentioned that their entities are prepared to deal with cyber threats **[44]**. A report by Bitdefender also revealed that the Iranian APT group targeted air transport and public entities in Kuwait and Saudi Arabia **[45]**.

These events have played a crucial role in renewing Cybersecurity concerns of the Saudi Kingdom and have made Saudi Arabia determined to improve its Cybersecurity in the future. As a result, Cybersecurity readiness has become a key performance indicator for transformation initiatives throughout the Kingdom **[46]**. The Saudi Kingdom has taken

major steps to mitigate future exposure to Cybersecurity threats and to enhance and develop its own Cybersecurity capabilities. This has led Saudi Arabia to achieve the world's second position in the Cybersecurity Index according to the 2022 Annual Report on Global Competitiveness issued by the Global Competitiveness Center.

According to the report, the most prominent factors that contributed to this achievement were:

- Establishing the National Cybersecurity Academy
- Implementing Cybersecurity training programs and exercises
- Launching business accelerators to support startups in the Cybersecurity field
- Issuing regulatory frameworks to support the development of Cybersecurity personnel
- Effective governance of the Cybersecurity system
- Providing a robust legislative environment for the Cybersecurity sector **[47]**.

Enhancing and Developing Cyber Capabilities at the Regional Level

Developing cyber capabilities at the regional level primarily relies on participating in international events, partnerships, investment agreements, and cooperation memoranda with regional states and worldwide in exchanging information and expertise, as well as combating and monitoring cyber-attacks.

The following were the most important steps taken by Saudi Arabia in enhancing and developing its cyber capabilities at the regional level:

- In September 2013, the Saudi Cabinet approved the implementation of the unified "Law" for combating information technology crimes for the GCC Countries **[48]**.
- On February 9, 2017, Saudi Arabia participated in the first meeting of the Permanent Committee for Cybersecurity in the GCC **[49]**.
- On Tuesday, March 29, 2022, the Saudi Cybersecurity and Programming Federation signed a memorandum of understanding with the Arab League Educational, Cultural, and Scientific Organization (ALECSO) to cooperate in the field of Cybersecurity **[50]**.
- In April 2022, the Saudi National Cybersecurity Authority signed a memorandum of understanding with the General Secretariat of the GCC to enhance cooperation between the two sides in various Cybersecurity-related issues **[51]**.
- On July 26, 2022, Saudi Arabia, represented by the National Cybersecurity Authority, chaired the seventh session of the Permanent Committee for Cybersecurity in the GCC **[52]**.
- On October 23, 2022, Saudi Arabia, with the participation of specialized bodies in the field of Cybersecurity in the GCC countries, conducted the "Gulf

Cybersecurity Exercise" on the sidelines of the first ministerial meeting for Cybersecurity in the GCC **[53]**.

Secondly: Impact of the Israeli-Iranian Cyberwar on Patterns of amity-enmity in the Arab Region

Until the beginning of the new millennium, the prevailing pattern of international relations between Arab States and Israel has historically been characterized by hostility. This was due to the catastrophe of 1948 and its aftermath of the establishment of the Israeli state on the occupied Palestinian territories. Despite the varying degrees of hostility between Israel and individual Arab States, the official Arab position has been unified in this regard. Peace and normalization of relations with Israel were linked to several decisive conditions, most of which were considered impossible for Israel to implement, including full withdrawal from occupied Arab territories and the return of refugees. This was reflected in the most flexible Arab initiative ever, the Saudi peace initiative launched by King Abdullah bin Abdulaziz, and adopted unanimously by the Arab summit held in Beirut in 2002 **[54]**.

On the other hand, it is likely that the historical pattern of enmity between Iran and Saudi Arabia, and the fact that Saudi Arabia is one of the most important strategic allies of the United States in the region, was one of the reasons for expanding the front of the Israeli-Iranian cyberwar by Iran to include vital Saudi targets **[55]**.

Today's Friends are Yesterday's Enemies

In a study published in 2019 titled “Facilitating Conditions of Saudi Arabia–Israel Normalization in 2015-2018” **[56]** the researchers observed a set of conditions created to facilitate efforts for normalizing relations between Saudi Arabia and Israel during 2015-2018. Among the most important of these conditions were:

- A change in the language of Saudi Crown Prince Mohammed bin Salman, indicating his desecuritization of the Israeli threats to Arab regional security.
- An increase in Iran's geopolitical influence, which made the conditions necessary for normalization extremely important.

The researchers argued that during that period, Saudi Arabia was the party that did not stop expressing the possibility of achieving normalization of relations between the Arab world and Israel. The achievement of the Neom project requires a good relationship with Israel because of the geographical location of the project and also because of Saudi Arabia's need for the technology that Israel possesses.

On the other hand, the hostile position of Saudi Arabia towards Iran has not been extinguished since the Iranian revolution in 1979. Saddam Hussein's retreat in Iraq and the Arab Spring led to increased enmity between the two countries. Also, Israel's hostility towards Iran was due to its involvement in the Israeli war in Lebanon. Both

Saudi Arabia and Israel have one goal, which is to suppress Iran's influence in the Middle East. Therefore, Saudi Arabia and Israel are concerned about the same security threat.

Abraham Accords

Abraham Accords refer to a new era of Arab-Israeli relations that began on September 15, 2020, when the United Arab Emirates and Bahrain established diplomatic relations with Israel. The goal of Abraham Accords is to maximize shared interests and address security issues by forming a new front against Iranian threats. As a result, cooperation between Israel and Gulf countries has become more visible than ever, particularly in cyberspace, where they share a common enemy. Through this new partnership, Gulf countries will benefit from Israel's advanced cyber capabilities in securing their vital infrastructure against Iranian threats, while opening up their lucrative markets to Israeli Cybersecurity companies. As a result, joint technical cooperation and information exchange will enable both sides to better address Iranian cyber activities.

Over the past decade, Gulf countries have quietly collaborated with Israel in the field of Cybersecurity. For example, according to former Israeli Knesset member Erel Margalit, Israeli Cybersecurity companies helped Saudi Arabia repair the damage caused by the cyber-attack on Aramco, which destroyed about 30,000 workstations and formed the largest commercial cyber-attack at the time **[57]**. In 2019, Bahrain invited a senior Israeli official to attend a security conference to discuss possible ways to form an alliance against Tehran's interventions in the region **[58]**. According to the Jerusalem Post, Israeli companies are secretly negotiating with the Saudi Public Investment Fund on possible ways to exchange expertise and technical skills necessary to complete the Saudi smart city of Neom **[59]**.

Therefore, it can be inferred that the increase in cyber-attacks against the targets of GCC countries and Saudi Arabia in particular has accelerated the process of establishing a cooperative framework between them and Israel aimed at enhancing alignment and coordination to address potential cyber threats through the exchange of information, technology, and expertise in the field of cyber security. This has resulted in a significant shift in the pattern of amity-enmity between the GCC and the Saudi Kingdom on the one hand, and Israel on the other, as they have all formed a united front against Iran.

In contrast, another cyber alliance was formed in the region between Iran and Russia. On January 26, 2021, Iran and Russia signed a joint cooperation agreement in the field of cyber security, including the transfer of technology, training, information exchange, and bilateral cooperation during international events **[60]**. Through the agreement, Russia can provide Iran with cyber defense systems and training to address its defense shortcomings, making potential cyber-attacks against Iranian targets more costly and difficult in the future. In addition, Iran can provide Russian technologies to its proxies in the region, such as Hezbollah and the Houthi militia, which can be used against Gulf or Israeli targets. Finally, Russian cyber teams can be sent to Iran to monitor Iranian

networks and examine American or Israeli malicious software used against Iran, helping both countries to enhance their defensive capabilities against future attacks **[61]**.

Thirdly: Impact of the Israeli-Iranian Cyberwar on Balance of Power in the Arab region

After the Stuxnet attack, which exposed the weakness and vulnerability of the Iranian cyber security system, Iran developed its cyber capabilities, and during the following decade, managed to respond to the United States and Israel **[62]**. With improved cyber security systems of their own, Iranian hackers increasingly targeted Gulf States with less protection. Iranian internet experts also trained infiltrators among their agents and encouraged them to launch attacks against their enemies. In 2015, the Yemeni cyber army targeted the Saudi foreign minister and leaked classified documents to Iranian media **[63]**. This indicates a shift in balance of the cyber power in the Middle East region in favor of Iran.

The Arab cyberspace has always been an open theater for cyber-attacks. The emergence of technological and digital capabilities in Arab Gulf states has opened up new vulnerabilities that have attracted many cyber-attacks. Despite the strenuous efforts made in developing cyber capabilities, Gulf States were not able until recently to develop a comprehensive cyber security system to protect government structures, vital facilities, companies, and individuals from such threats. For example, according to a 2017 report by the Potomac Institute, Saudi Arabia "remains insufficiently prepared in all essential elements of cyber readiness" **[64]**. The Saudi national information security strategy failed to provide specific guidance and a consistent structure for cyber security. Often, many ministries, companies, and other entities developed their own cyber strategies independently, leading to serious gaps in national cyber security. Furthermore, with the COVID-19 crisis, cyber threats increased with the proliferation of phishing attacks and malware. In such an environment, Gulf States needed experienced partners to enhance their cyber security systems **[65]**.

On the other hand, Gulf States have realized that Israel is the most advanced country in the Middle East in terms of Cybersecurity. The CEO of the Emirati Cybersecurity Company DarkMatter stated that "the only country in the region that has strength in Cybersecurity is Israel" **[66]**.

Therefore, obtaining Israeli expertise in intelligence and cyber security (even before Abraham Accords) was an important factor in bringing positive changes to the balance of cyber power in the Arab Region and reducing the Cybersecurity weaknesses of GCC. Israel and GCC countries officially claimed that their cooperation aims to counter Iranian threats in cyberspace. However, GCC countries have been and continue to seek to benefit from Israeli expertise to enhance their own Cybersecurity capabilities **[67]**.

In the end, it is likely that Israeli cooperation with GCC countries in Cybersecurity will lead to a significant change in the balance of Cyber power in the Arab region.

Conclusions

Results show that Saudi Arabia and GCC countries constitute a regional Cybersecurity complex according to the "Regional Security Complex Theory", which states that security dynamics, including threat construction, can operate at a regional level among certain groups of states. In these cases, Buzan and Waever argue that those states form a "regional security complex", where their security visions are interconnected even if not all members of the regional security complex agree on security threats **[68]**.

This study proves that this approach can be applied to Cybersecurity by forming a "regional Cybersecurity complex". The initial drawing of such a complex shows that Saudi Arabia and GCC countries constitute a regional Cybersecurity complex, where each is exposed to significant cyber operations and possesses a range of Cybersecurity structures and capabilities. They also have a common enemy representing a continuous threat to them in cyberspace; Iran, and a common strategic ally providing them with support; Israel.

Considering the factors that the Regional Security Complex Theory identified as conditions for achieving such a pattern of international relations between several states, we find that the Israeli-Iranian cyberwar has undoubtedly contributed to the formation of a regional Cybersecurity complex between Saudi Arabia and GCC countries, where:

Firstly, Cybersecurity threats resulting from repeated attacks on the capabilities of GCC and Saudi Arabia pushed them to develop their Cybersecurity capabilities internally. After suffering from being behind in international Cybersecurity rankings, Saudi Arabia now ranks second globally, according to the latest international reports.

Additionally, Saudi Arabia has also strengthened its Cybersecurity capabilities at the regional level and has signed several joint cooperation agreements with regional and international allies. It has also managed and participated in several regional and international Cybersecurity events, demonstrating its growing Cybersecurity prowess and led the GCC countries in a cyber-security bloc under the name "Permanent Committee for Cyber Security in the GCC Arab States".

This represents a positive change in mutual Cybersecurity dependence between Saudi Arabia and the GCC countries. The main motivation for such a change was the cyber-attacks that Saudi Arabia and GCC countries suffered during the Israeli-Iranian cyber war, carried out by one of the parties involved in that war; namely Iran.

Secondly, changes in patterns of amity-enmity in the region were inevitable, especially with the cyber capabilities possessed by one of the parties involved in the Israeli-Iranian cyber war; namely Israel. Israel has not, and still does not; pose a direct security threat

to Saudi Arabia and the Gulf Arab states in the cyber domain. Indeed, much cooperation has taken place between the two sides over the years leading up to the Israeli-Iranian cyber war, particularly in the field of cyber security.

Despite the obstacles created by the Palestinian-Israeli conflict that prevented full normalization of relations between Arab countries and Israel, the Saudi Kingdom believed it was possible to desecuritize the threats or concerns created by the Palestinian issue, in order to bring about closer relations with Israel, at least in the field of Cybersecurity. Some Gulf countries have taken a more advanced approach to enhancing cooperation between them and Israel by signing Abraham Accords. This has brought about a significant change in the patterns of amity-enmity in the Arab region.

Thirdly, the positive change in Saudi Arabia's cyber defense and deterrence capabilities has caused a significant shift in the balance of cyber power in the Arab region. The Arab region was previously vulnerable to cyber-attacks from individuals and states, this weakness may have prompted Iran to carry out cyber-attacks on Saudi Arabia's capabilities, causing damage to the strategic interests of the United States, one of the parties involved in the Israeli-Iranian cyberwar, by attacking one of its key allies in the region.

Currently, GCC countries, particularly Saudi Arabia, possess cyber defense and deterrence capabilities that are ranked second globally by international institutions. They also have Cybersecurity cooperation and coordination links with the United States and Israel, which are both enemies to Iran.

This tangible change in the balance of cyber power in the Arab region serves as a strong deterrent to Iran and other states or groups that may be considering a cyber-attack on Saudi Arabia and/or the GCC countries. Recent reports have even noted a significant decline in cyber-attacks on the Gulf region and on Saudi Arabia in particular **[69]**.

Therefore, it can be said that the Israeli-Iranian cyberwar had a clear impact on the Arab regional security. The aftermath of that war and the dangers and threats it left behind resulted in fundamental changes in the patterns of international relations in the region. In particular, it led to:

- Increasing mutual Cybersecurity dependence
- Changing the patterns of amity-enmity
- Changing the balance of cyber power among the countries of the region.

This finally resulted in the formation of an Arab regional Cybersecurity complex, at the initiative of the Kingdom of Saudi Arabia with participation from the Gulf Cooperation Council countries.

Recommendations

Based on the previous results, the researcher recommends the following:

1. The Saudi Kingdom has achieved rapid advances in the field of cyber readiness, but there is a noticeable disparity in the cyber readiness efforts of other GCC countries. Therefore, the governments of GCC countries should commit to a sustainable commitment to cyber resilience that provides clear guidance for organizations and businesses and achieves the best use of emerging Cybersecurity frameworks. This may require more participation in initiatives with regional and international partners to enhance cyber readiness.
2. The activities of the Regional Cybersecurity Complex formed by the Saudi Kingdom with the GCC countries should not be limited to dealing with cyber threats within its narrow geographic scope, but its security umbrella should extend to cover the entire Arab region from the ocean to the Gulf, through including all Arab League member states in its activities, events, and agreements.
3. All Arab States should join a common platform aiming to put each country at a similar level of cyber readiness according to uniform standards. This role is best played by the Arab Information and Communication Technology Organization AICTO, which is one of the specialized organizations established by the Arab League.
4. Arab countries must exercise a great deal of caution in dealing with Israel in the field of Cybersecurity and should never be deceived by exaggerated claims of Israel's cyber capabilities. The Israeli-Iranian cyberwar revealed clear weaknesses in the Israeli cyber security system, which allowed Iran to carry out painful cyber-attacks against Israel.
5. Arab decision-makers should be aware that opening Arab markets to Israeli Cybersecurity companies necessarily means giving Israel a copy of the keys to Arab data vaults. History teaches us that nothing comes without a price, especially when dealing with an occupier who has shown extreme ferocity and unparalleled stubbornness over more than 50 years of the Arab-Israeli conflict.
6. In the field of education and scientific research, Arab countries must expand the creation of smart cities and technology parks, which provide a common space for scientific research, and investment cooperation among government officials, academics, and business people. This will enhance the cyber readiness of society as a whole through collaborative research in Cybersecurity projects.
7. It is also important to design special educational programs that aim to train Arab students in all educational stages on exceptional Cybersecurity skills, to ensure that Arab cyber companies and research centers are supplied with qualified human resources.
8. In the technical field, all Arab countries must ensure a reasonable level of technology dissemination among their populations, not less than the global average, by investing in high-speed internet connections, providing schools and universities with advanced computer labs, and expanding digitization programs of government services, while not neglecting the cyber readiness required for such expansion.

9. In the political field, the Arab League should establish a binding framework for all Arab countries to regulate Cybersecurity partnership and cooperation agreements between Arab and non-Arab countries. This framework should ensure secure data exchange that does not endanger Arab regional security from espionage, hacking, and sabotage.
10. Arab countries that are willing to develop their Cybersecurity capabilities should realize that transparency, freedom of speech, and Freedom of Information for Arab peoples, are essential and decisive factors that provide the motivation for all segments of society to participate effectively in the process of developing Cybersecurity capabilities. This guarantees the awareness of all segments of society about Cybersecurity risks and how to deal with them at all levels.

References

[1] Abbas N., 2018, “Arab Countries Facing the Highest Number of Cyber Attacks”. Forbes Middle East, 28 March, accessed 10 March 2023, https://bit.ly/3doronD
[2] Afp, 2012, US thinks Iran behind cyberattack in Saudi: ex-official, The Express Tribune, 13 October, accessed 10 March 2023, https://bit.ly/3dy2rWM
[3] Osgood, P., 2012, Cyber attack takes Qatar’s RasGas offline, Arabian Business, 30 August, accessed 10 March 2023, https://bit.ly/30dz4Gi
[4] Afp, 2012, op. cit.
[5] Sardarizadeh S., 2016, Iran-Saudi tensions erupt in 'cyberwar', BBC, 3 June, accessed 10 March 2023, https://bbc.in/3dxaSBP
[6] Buzan B., 2007, People, states & fear: An agenda for international security studies in the post-cold war era (2nd ed.), Colchester, UK: ECPR Press
[7] Buzan B., 1988, The Southeast Asian security complex. Contemporary Southeast Asia, 10(1), 1–16.
[8] Morgan, P.M., 1997, Regional security complexes and regional orders. Regional orders: Building security in a new world, pp.20-42
[9] Buzan B., Wæver O., & de Wilde J., 1998, Security: A new framework for analysis. Boulder, CO.: Lynne Rienner, p. 17
[10] Buzan B., Wæver O., & de Wilde J., 1998, op.cit. p. 168
[11] Andžāns M., 2015, Prospects of Regionalization of Security in the Cyberspace: Case of the Baltic States, Proceedings of the Conference of Turiba University, XIV International Scientific Conference “Creating the Future: Communication, Education, Business", pp. 20-21
[12] Rainie L., Anderson J., & Connolly J., 2014, Cyber Attacks Likely to Increase, Pew Research Center, 29 October, accessed 10 March 2023, https://pewrsr.ch/3JJbIt8
[13] Lukman E., 2013, Tech in Asia - Connecting Asia’s Startup Ecosystem, www.techinasia.com, 11 November, accessed 10 March 2023, https://bit.ly/36JJZKY
[14] Dwinanda R., 2018, BSSN to Team up with Australia to Deal with Cyber Attacks, Republika Online, 1 February, accessed 10 March 2023, https://bit.ly/3MrIRLh
[15] Department of Foreign Affairs and Trade, 2018, Memorandum of Understanding between the Government of the Republic of Indonesia and the Government of Australia on Cyber Cooperation, accessed 10 March 2023, https://bit.ly/3Lnp6Ve

[16] Lestari, E.A.P., 2021, Complex Interdependence Between Indonesia-Australia Through Cybersecurity Cooperation Post-Indonesia-Australia Cyberwar in 2013, Jurnal Hubungan Internasional, 9(2), pp.178-188. https://doi.org/10.18196/hi.v9i21.10522
[17] Government of Estonia, 2008, Cyber Security Strategy, Ministry of Defence, p. 6, accessed 10 March 2023, https://bit.ly/3MC5M6v
[18] Government of Estonia, 2008, op.cit. pp. 10-21
[19] European Union Agency for Cybersecurity, 2014, Cyber Security Strategy Of Latvia 2014-2018, enisa.europa.eu, European Union Agency for Cybersecurity, p. 2, accessed 10 March 2023, https://bit.ly/3ydaPqr
[20] Government of Lithuania, 2011, the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019. enisa.europa.eu, European Union Agency for Cybersecurity, p. 1, accessed 10 March 2023, https://bit.ly/3OIGIwM
[21] Concordiam P., 2016, Baltic Cyber Cooperation: Estonia, Latvia and Lithuania Sign a Historic Document to Align Their Cyber Defense Policies, 14 July, accessed 10 March 2023, https://bit.ly/3xRnmj0
[22] Andžāns M., 2015, op. cit. pp. 14-24
[23] Setyawati, S.M.A. and Agussalim, D., 2015, security Complex Indonesia-Australia dan Pengaruhnya terhadap Dinamika Hubungan Kedua Negara, Jurnal Ilmu Sosial dan Ilmu Politik, 19(2), pp. 111-124
[24] Dwinanda R., 2018, op. cit. And
Department of Foreign Affairs and Trade, 2018, op. cit.
[25] Engel D., 2021, Australia–Indonesia relations: Keeping It Real, The Strategist, 23 February, accessed 10 March 2023, https://bit.ly/3kn425i
[26] Concordiam P., 2016, op. cit.
[27] Andžāns M., 2014, Securitization in Defining Regional Security Complexes: the Case of the Baltic States (2004–2013), Summary of the Doctoral Thesis
[28] Buzan B. and Wæver O., 2003, Regions and powers, Cambridge, UK: Cambridge University Press, p. 435
[29] Prucková M., a 2022, Regional Security Complex Theory and the Baltic states. How Have Their Relations with the Russian Federation Changed after the Bronze Year 2007 incident? Security Outlines, 23 March, accessed 10 March 2023, https://bit.ly/3L5qjzr
[30] Rojčík O., 2019, "Achievements and Failures of NATO Cyber Policies", In NATO at 70: Outline of the Alliance Today and Tomorrow, edited by R. Ondrejcsák, T. H. Lippert, 179-192. Bratislava: STRATPOL
[31] Prucková M., b 2022, Cyber Attacks and Article 5 – a Note on a Blurry but Consistent Position of NATO, ccdcoe.org, accessed 10 March 2023, https://bit.ly/3FJ6qgr
[32] Rhodes E., 2000, The American Vision of Baltic Security Architecture: Understanding the Northern Europe Initiative, Baltic Defence Review, 4, pp.91-112, accessed 10 March 2023, https://bit.ly/3w6jnOl
[33] Bergmane U., 2020, Fading Russian Influence in the Baltic States, Orbis 64(3), pp. 479-488
[34] Gorenburg D., 2019, Russian Strategic Culture in a Baltic Crisis, George C. Marshall European Center for Security Studies, March, accessed 10 March 2023, https://bit.ly/39cgySy
[35] Bergmane U., 2020, op. cit.
[36] Prucková M., a 2022, op. cit.
[37] Seeger R. & Thafer D., 2018, "The New Battlefront: Cyber Security across the GCC – Gulf International Forum." Gulfif.org, 29 October, accessed 10 March 2023, https://bit.ly/3XNimWW
[38] ITU, 2013, MEASURING THE INFORMATION SOCIETY 2013, op.cit. And

Bilbao-Osorio B., Dutta S. & Lanvin B., 2014, Insight Report: the Global Information Technology Report 2014, Rewards and Risks of Big Data, World Economic Forum, accessed 10 March 2023, https://bit.ly/3verZ5v. And
ABI Research, 2014, GLOBAL CYBERSECURITY INDEX. ITU, op.cit.
[39] Ghernaouti-Hélie S., 2008, From risk management to information security policies and practices: a multi perspective framework for ICT security effectiveness. Geneva: International Telecommunication Union, 14 April, accessed 10 March 2023, https://bit.ly/3vdfWoO
[40] Abbas N., 2018, op. cit.
[41] Fazzini K., 2019, "The Saudi Oil Attacks Could Be a Precursor to Widespread Cyberwarfare — with Collateral Damage for Companies in the Region." CNBC, 21 September, accessed 10 March 2023, https://cnb.cx/3U8JWfj
[42] al-Hussein I., 2017, "60 Million Cyber Attacks Targeted Saudi Arabia in One Year." Al Arabiya English, 2 May, accessed, 10 March 2023, https://bit.ly/3UnOs9k
[43] Tashkandy H., 2020, Cyberattacks hit 95% of Saudi businesses last year, says study, Arab News, 12 August, accessed 10 March 2023, https://arab.news/j4pt5
[44] Guzansky Y. & Deutch R., 2019, How Prepared is Saudi Arabia for a Cyber War? INSS Insight No. 1190, 10 July, accessed 10 March 2023, https://bit.ly/3icsOHl
[45] Arsene L., 2020, Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia, bitdefender.com, 21 May, accessed Nov 5, 2022, http://bit.ly/3u4SHvv
[46] IDC, 2020. "Cybersecurity and its impact on digital Saudi" idc.com, accessed 10 March 2023, https://bit.ly/3E4A68y
[47] Saudi Press Agency, 2022, Saudi Arabia Ranks Second Globally in Cybersecurity Index According to World Competitiveness Yearbook 2022, SPA, 15 June, accessed 10 March 2023, http://bit.ly/3Z9akY8
[48] Aissani R., 2022, Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. Journal of Legal, Ethical and Regulatory Issues, 25(1), 1-14
[49] Alkhaleej Online, 2017, 1st meeting of the Gulf Committee for Cybersecurity was held in the UAE, (Arabic) 10 February, accessed 10 March 2023, https://perma.cc/TZL3-XDEQ 2022
[50] Saudi Federation For Cybersecurity, Programming & Drones, 2022, SFCPD & ALECSO face informational risks in the Arab world (Arabic), 29 March, accessed 10 March 2023, https://safcsp.org.sa/news-elexo
[51] DataGuidance, 2022, International: NCA signs MoU with General Secretariat of Cooperation Council for Arab States of the Gulf, 22 April, accessed 10 March 2023, http://bit.ly/3LKJvq9
[52] Saudi Press Agency, 2022, Saudi Arabia Chairs Standing Committee's Meeting on GCC Cybersecurity, SPA, 28 July, accessed 10 March 2023, http://bit.ly/42EEd5l
[53] Saudi Press Agency, 2022, GCC Ministerial Committee for Cybersecurity Launches 1st Gulf Cybersecurity Exercise, SPA, 23 October, accessed 10 March 2023, http://bit.ly/40cgJTC
[54] Reuters Staff, 2020, Saudi remains committed to Arab Peace Initiative for Israel peace, foreign minister says, Reuters, 19 August, accessed 10 March 2023, http://bit.ly/3nljQKv
[55] BBC Monitoring, 2017, Iran and Saudi Arabia: Friends and foes in the region, BBC News, 10 November, accessed 10 March 2023, http://bit.ly/3U5jIcF. And
Guzansky Y. & Deutch R., 2019, op. cit.
[56] Jamilah M., Fikra H.U., & Harza Z., 2019, Facilitating Conditions of Saudi Arabia–Israel Normalization in 2015-2018, Journal of Diplomacy and International Studies, 2(01), pp.38-51
[57] Hirschauge O., 2017, Former Israeli Parliamentarian Says Homegrown Companies Can Help Build Saudi Future City Neom, calcalistech.com, 21 November, accessed 10 March 2023, http://bit.ly/3GW7dx0

[58] Reuters Staff, 2019, Senior Israeli official attends Bahrain security meeting focusing on Iran, Reuters, 21 October, accessed 10 March 2023, http://bit.ly/3iem1gq
[59] Schindler M., 2017, Israeli companies working with Saudi Arabia? The Jerusalem Post, 26 October, accessed 10 March 2023, http://bit.ly/3EIdlGy
[60] Russian News Agency, 2021, Russia, Iran sign agreement on cyber security cooperation, TASS, 26 January, accessed 10 March 2023, https://tass.com/politics/1248963
[61] Wechsler O., 2021, The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East, Council on Foreign Relations. 21 March, accessed 10 March 2023, https://bit.ly/3XwZJXf
[62] Work J. & Harknett R., 2020, troubled vision: Understanding recent Israeli–Iranian offensive cyber exchanges. Atlantic Council, 22 July, accessed 10 March 2023, http://bit.ly/3XAtXZl
[63] Sputnik International, 2015, Yemeni Hackers Reveal Top Secret Docs in Saudi Government Cyber Attack, 22 May, accessed 10 March 2023, https://sputniknews.com/20150522/1022475567.html
[64] Hathaway M., Spidalieri F., & Alsowailm F., 2017, Kingdom of Saudi Arabia cyber readiness at a glance, Potomac Institute for Policy Studies, accessed 10 March 2023, https://bit.ly/3VmrK2b
[65] Alexander K., 2020, "Israeli-Gulf Cyber Cooperation." Modern Diplomacy, 23 December, accessed Nov 30, 2022, https://bit.ly/3UluVpu
[66] Fenton-Harvey J., 2019, "UAE-Israel Cyber-Spying Aids Emirati Influence, Repression." Inside Arabia, 27 December, accessed 10 March 2023, https://bit.ly/3uehUn7
[67] Alexander K., 2020, op. cit.
[68] Buzan B. & Wæver O., 2003, op.cit. p. 435
[69] Banda M., 2022, "Latest Data Shows Saudi Arabian Organisations Making Gains in Building Greater Cyber Resilience." Intelligent CIO Middle East, 20 July, accessed 10 March 2023, https://bit.ly/3uphQkJ

Dedication

To my mother, Mrs. Nadia Khalaf Abdulhafiz: the Egyptian girl who grew up in Tema, one of the poorest cities in Upper Egypt, and lived a miserable childhood suffering from poverty, and family disintegration. After being prevented from completing her basic education due to poverty, she defied all societal constraints and borrowed fifty piasters to complete her basic education, then joined the midwifery training program at Qena Central Hospital where she excelled and became the first in her class.

Despite the cruelty of social constraints, she succeeded in achieving independence in her life, starting our small family, completing her education, and having a successful professional record as a nurse for more than 42 years.

She decided to change her painful reality armed with knowledge and determination, to carve her way in life among high mountains of illiteracy, poverty, and backwardness. She ignored defeatism, hatred, and bullying, and fought many battles filled with sacrifice and dedication just to survive with our small family ship to the safe shore.

To the honorable Mrs. Rad Al-Ruh, the headmistress of Girls Primary School in Tema, who lent my mother those fifty piasters in 1960.