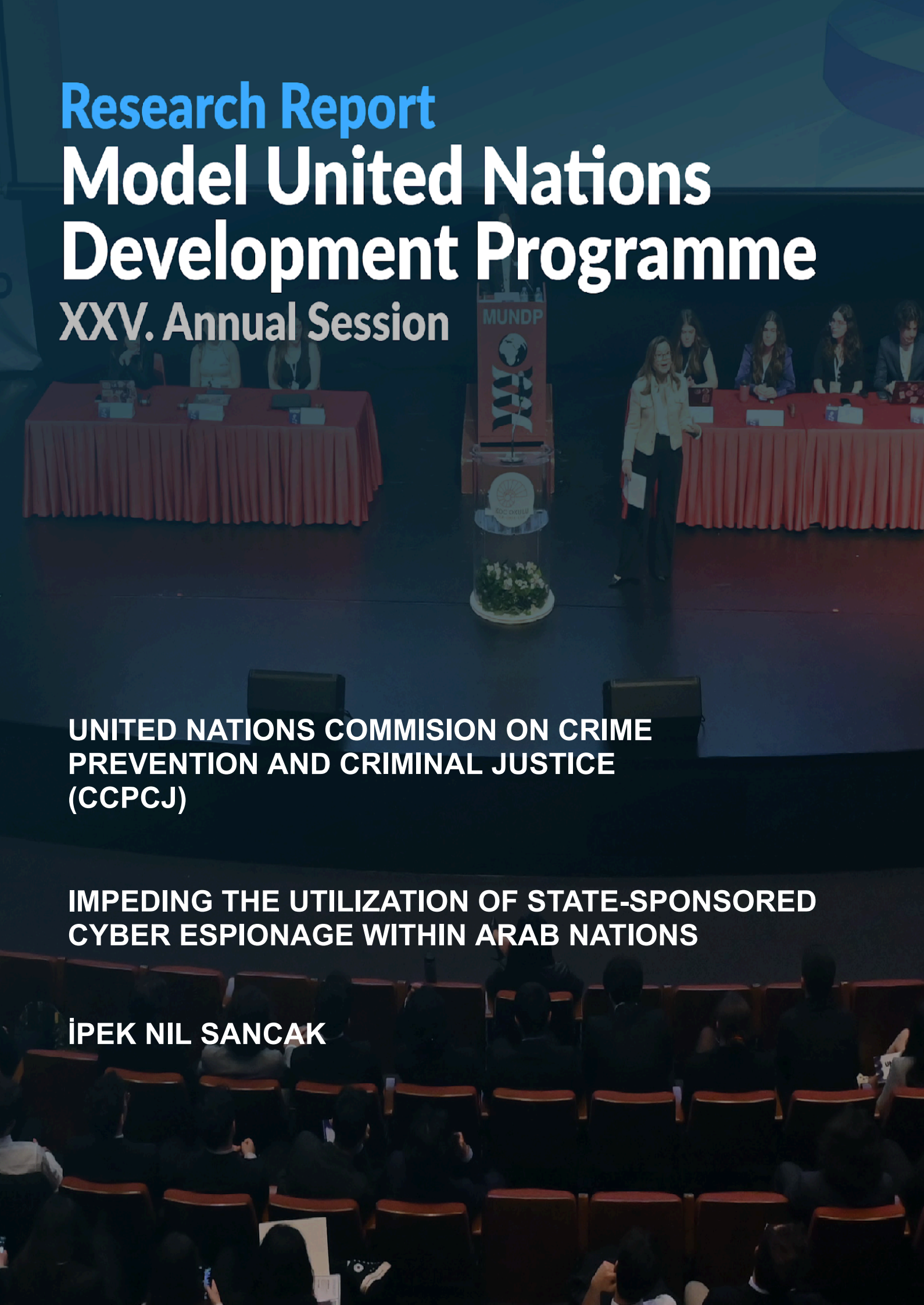

Research Report

Model United Nations Development Programme

XXV. Annual Session

UNITED NATIONS COMMISION ON CRIME PREVENTION AND CRIMINAL JUSTICE (CCPCJ)

IMPEDING THE UTILIZATION OF STATE-SPONSORED CYBER ESPIONAGE WITHIN ARAB NATIONS

İPEK NIL SANCAK

Basic Overview of the Issue

In today's world, when everything is interlinked, dependence on digital infrastructure and cyberspace has completely changed the political, economic, and security standards of the world. While the internet and technological advancements have opened new avenues for growth, communication, and innovation, they have also opened up new avenues for emerging threats such as cyber espionage. Of these, state-sponsored cyber espionage has emerged as a top threat that especially comes across the Arab Nations, whose geopolitics and regional vulnerabilities make them a field for exploitation.

Cyber espionage is the indication of a secret intrusion into systems and networks, theft of sensitive information, or disruption of critical infrastructures using cyber instruments and tech. It involves sophisticated operations organized by state actors to get hold of any strategic objectives such as political leverage, economic advantage, and military advantages over others.

The Arab nations face a unique set of challenges in countering cyber espionage because they comprise diverse political systems, economic capabilities, and levels of technological development. Most regional key industries, like oil production, finance, and transportation, have been highly dependent on digital technologies, so the region's critical infrastructure has become one of the main targets of cyberattacks. Furthermore, ongoing conflicts and rivalries, along with political instability, increases the risks associated with state-sponsored cyber activities.

Various factors contribute to the vulnerability of the Arab Nations to cyber espionage. For one, the rapid digital transformation that is happening in most countries often runs ahead of setting up strong and durable cybersecurity frameworks. Without standardized cyber defense policies and intergovernmental coordination, many gaps exist that could be exploited by state actors. Second, the high dependence on foreign technology and software makes the risk of backdoor access and supply chain vulnerabilities greater, thus allowing malicious entities to interfere and exploit the network undetected. Lastly, limited awareness and preparedness in order to address emerging cyber threats make the region all the more vulnerable to cyberattacks.

The implications of state-sponsored cyber espionage in the Arab Nations are wide-ranging. Economically, it puts at risk key industries and disrupts trade by targeting supply chains and financial systems. Politically, it undermines sovereignty and stability through the manipulation of elections. Socially, it destroys and highly damages trust in governments and institutions, further shredding already fragile societies. To respond to these challenges, there is a need for regional cooperation and strict cybersecurity measures.

Thus, the question of cybersecurity has come to the forefront within international organizations and regional alliances during the last decade. Meanwhile, comprehensive measures concerning the deterrence of state-sponsored cyber espionage remain inadequate. Certain measures to diminish cyber threats do exist, including the creation of cybersecurity task forces, enactment of data protection laws, and tightening public-private partnerships. Moreover, international cooperation through frameworks such as the United Nations' Group of Governmental Experts on Information Security enables the elaboration of norms and protocols to govern state behavior in cyberspace.

The Arab Nations need to be in a position where the threat of state-sponsored cyber espionage is recognized not only as a national security threat but also as a regional one.

Explanation of Important Terms

Cyber Espionage

The practice of using cyber tools, techniques, or related methods to secretly steal information or intelligence from governments, organizations, or individuals. It often encompasses network or device hacking in efforts to get sensitive data, most often for political, economic, or strategic ends. (Oxford Bibliographies, 2024)

Surveillance Tools

Software that monitors and collects data from devices without the user's consent. For example, Pegasus is spyware that can access calls, messages, and even turn on cameras and microphones. These tools are used by governments for security and political purposes.

Proxy Actors

Non-state actors, such as hacktivists or criminal organizations, usually supported or tolerated by states that can deny involvement in the cyber activities of these sponsoring

states. These actors are common in regional cyber conflicts.

Cybersecurity

Cybersecurity is the protection of systems, networks, devices, and data from digital destruction, theft, and other harming events that may occur.

Digital Infrastructure

Digital infrastructure includes technologies, systems, and frameworks that allow digital operations, communication, and services. It forms the backbone of modern digital ecosystems, from simple devices through to complex global business operations.

State-Sponsoring

State-sponsoring is the act of aiding a project or an action financially, politically or physically as a national government. State-sponsored matters are usually dealt with by the national governments of countries, meaning that they are backed by an official member of the United Nations. Contrary to private initiatives, state-sponsored projects are not conducted by individuals, thus making them accountable to a whole nation.

Digital Sovereignty

Digital sovereignty is a term that has emerged after the rise of the internet. Sovereignty refers to the right of a state to remain independent from other nations while restricting any foreign interventions that are not authorized by the nation itself. Digital sovereignty is broken when the digital databases and security systems of a country are breached through the utilization of cyber espionage, hacking or other digital crimes.

Digital Transformation

Digital transformation is the change in a country's technological development status. This usually occurs because of economic growth in a country when the national government opts to invest more in the development of digital technology.

Detailed Background of the Issue

State-sponsored cyber espionage has become a notable issue across the globe and its history and evolution within the Arab states has had direct relations to the social, political and economic atmosphere of the region. Cyber espionage in the Arab region cannot be fully

comprehended without first understanding the role of the global cyber espionage adaptation that preceded it, as it led to the eventual regional use of the cyber tools. Beginning in the 1980s with activities such as the KGB hack, which saw German hackers gain access to American systems and sell the information to the Soviet Union, cyber espionage operations started to emerge in the US. These practices demonstrated that digital devices had strategic capabilities for collecting intelligence, which invited countries all over the world including the Arab world to start experimenting with such technology and integrating it into their institutions responsible for national security.

Rise of Technology in the Middle East

During the last two decades of the twentieth century and the first two decades of the twenty first century where internet construction increased in several Arab nations, there was this growing realization within the governments of these states of the toasty nature of the cutting edge transformation. The Internet outburst represented new opportunities for development, growth and people connectivity, but at the same time made critical infrastructure vulnerable. Saudi Arabia, the United Arab Emirates (UAE), and Doha, among other Gulf Coastal states, embarked first on protective but also defensive advanced cybersecurity steps in order to secure key business sector assets such as oil and gas. Towards the mid-2000s, the use of cyber technologies extended beyond benevolent use, as they were being used for intelligence purposes. They have been also utilized for endeavors of regional power struggles, which demonstrates the menace the Arab States face because of the rivalry in the Middle East.

Foreign Interference

A major implication of US and Russia’s interference in Arab states is the determination of the cyber landscape in Arab states. The two countries have both utilized the region as a proxy for their own cyberspace wars. For example, Russian cyber operatives targeted the Assad regime as the cyber operations were conducted during the time of the Syrian civil war. The region was at the receiving end of US cyber operations that were aimed at ISIS. Moreover, the two great powers have been able to foster relations with Arab states based on cybersecurity. For instance, the UAE has expressed interest in availing the services and expertise of US cybersecurity firms. Former NSA operatives were even employed as part of

Project Raven, an undercover program aimed at surveillance and cyber initiatives, in an attempt to grasp an edge over Islamic extremism. On a similar note, Russia has given cyber capabilities to its partners like Syria and Iran, shaping the policies at an Arab state level due to the geopolitical climate.

In relation to cyber espionage, spyware such as Pegasus, created by Israel's NSO group, has been enough fuel to the fire in the already burning region. Due to its growing popularity across the region, it has been a major point of concern, especially regarding the ethics and legitimacy of such behavior in regards to targeting political activists, journalists, and foreigners. These tools acquired from other countries were used as a means to exercise authority and curtail insubordination which led to exacerbating the integration of cyber technology into the nation state and the process of nationalization of cyber capabilities.

International Insurgency

Cyber espionage has become another form of political rivalry among the Arab countries and it is more pronounced at times of political crisis. During the Gulf Crisis in 2017, Arab countries engaged in cyber warfare against each other. Hacking of the Qatar News Agency, which has fabricated statements of the Qatar Emir, was allegedly used by Dubai based operatives. The retaliatory cyber operations of Qatar against officials and infrastructure in other countries were acts of self-defense. Also, among the Arab newspapers, emails of the Emirate officials were leaked where they outlined a sensitive foreign policy strategy in an effort to choke the political crisis.

The conflict is not only confined to the Gulf region. In North Africa, the territorial conflict involving Western Sahara has contributed to cyber warfare between Algeria and Morocco. There are indications that each country has intruded into the government and critical infrastructures of the other. This ongoing digital conflict has made the region more polarized and shown that cyber warfare are means that can be employed in the pursuit of geopolitical goals within the Arab world.Saudi Arabia, United Arab Emirates and Qatar, for instance. These regions will always be leaders in cyber tools after implementing advanced frameworks. The cybersecurity market in Saudi Arabia alone is worth 500 million dollars controlled by the National Cybersecurity Authority of the country. In the UAE the advancement in cyberspace began in 2019 with their cyber strategy. In order to combat the

increased cyber threats due to the pandemic, which surged by 250%, the UAE developed a strategy in 2019 (ResearchGate, 2022).

These countries also participate in spying on their regional adversaries. Both Algeria and Morocco have a long history of disputing over Western Sahara territory, which has resulted in them resorting to hacking each other. UAE, during the 2017 Gulf crisis, hacked the Qatar News Agency, which helped escalate the diplomatic crisis between the two nations. These actions are detrimental to regional cybersecurity cooperation. To make matters worse, global governments tend to make this gap deeper as well. While the US supports its allies in the Gulf region, the Russians are propping up Syria and encouraging cyber activities with the aim of destroying Gulf-based infrastructure. Hundreds of thousands of computer attacks in the Shamoon cyberwar began when Saudi Aramco was attacked in 2012, targeting oil markets that supply more than 30% of the world's energy (Al Jazeera, 2019). With such devastating attacks, the risk of flooding Silicon Valley at $1 trillion is realistic. Pro-cyber warfare states engage in hostile actions that undermine regional security frameworks, and inaction only serves to perpetuate tensions. Efforts to counter the global reach of cyber espionage will require regional participation, respect for international law, and policy coherence.

Most of the cyber espionage in Arab states is greatly influenced by this interference from outer powers like the United States, Russia, China, and Israel, all using advanced cyber-attack capabilities in an attempt at influencing, political manipulation, or securing economic and strategic advantage. One prominent example could be the Iraq War, when the U.S. resorted to cyber operations with the aim of disconnecting insurgents from the ability to communicate, trace adversaries, and gain full control over the information networks-dropping the curtain to the future militarization of cyberspace in this region. With the appearance of this intervention came a huge surge in the growth of hacking tools and cyber-capability that have afterward been exploited through varied and numerous actors. In the case of Russia in Syria, Moscow has undertaken cyber operations to gain intelligence on opposition elements and support military action. China, meanwhile, is accused of utilizing cyber espionage against governments and infrastructure projects throughout the Arab world for economic intelligence in pursuit of its Belt and Road Initiative, implanting vulnerabilities in the long term.

Furthermore, Israel's highly developed expertise in cybersecurity contributed much to intelligence gathering, mainly against Iran and its proxies, and to developing spyware tools like Pegasus, which regional Arab governments employed to monitor activists, journalists, and political dissidents in places such as the UAE and Saudi Arabia.

These external interventions are a very serious issue for the Arabs. For example, Saudi Arabia has faced severe economic and reputational loss due to suspected Iranian attack, known as Shamoon malware on Saudi Aramco in 2012; this had erased data from thousands of computers. Events of this nature illustrate ways through which susceptibility to cyberspace would trigger huge shortfalls in heavy industries. The UAE's usage of Pegasus spyware had the effect of tampering regional diplomatic relations while exposing the greater risks associated with relying on foreign-made cyber tools that are often built with backdoors. Most egregious of all, though, is probably the murder of Jamal Khashoggi, whose activities were apparently tracked by Saudi Arabia through the use of spyware. More than these, the broader cyber capabilities misuse in Yemen in which Saudi-backed and Iranian-backed forces have used cyberattacks-inflamed that conflict and worsened its humanitarian crises.

It was the ultimate undermining of sovereignty, stability, and security in the region when the external powers and Arab governments used cyber tools against each other. Since such interventions have already become pervasive, it is time to adopt a common approach in strengthening cybersecurity, creating regulations on the use of surveillance tools, and establishing international norms to prevent further destabilization in this region.

Major Parties Involved

United States of America (USA)

The United States is among the most active actors in cyber espionage, leveraging huge technological capabilities through agencies such as the NSA and CIA. Very often, it is interested in tapping into international communication networks to monitor terrorism and safeguard its geopolitical interests. In the Arab region, the United States has been implicated in cyber activities related to conflicts like the Iraq War and has been both building and penetrating the cybersecurity of friendly nations.

China

China is infamous for state-sponsored cyber operations targeting infrastructure projects, intellectual property, and economic systems. The involvement of China in the Arab nations under the Belt and Road Initiative has brought up concerns about cyber espionage, with accusations of backdoors in technology systems provided to these countries.

Russia

Russia resorts to cyber instruments for intelligence collection, shaping public opinion, and undermining political stability in regions of strategic concern, including the Arab region. In Syria, for example, Russian cyber activities have complemented military action through surveillance, disinformation campaigns, and targeting opposition groups.

Israel

With its developed cybersecurity industry, Israel conducts cyber espionage mainly against perceived threats, primarily Iran and its proxies. It also has been linked to providing such tools as the Pegasus spyware, used by some Arab governments to conduct surveillance.

Iran

Iran is one of the well-known regional players heavily involved in cyber espionage against GCC states and other rivals. Attacks attributed to them include the critical infrastructure disruption Shamoon malware attack against Saudi Aramco, alongside using cyber capabilities for intelligence collection to retaliation.

Saudi Arabia

Saudi Arabia has been putting much effort into the protection of its critical infrastructure, such as its oil industry, through initiatives like the National Cybersecurity Authority. This also underlined the resilience of Saudi Arabia against external threats in response to these cyberattacks-for instance, the Shamoon malware by Iran that targeted Saudi Aramco. Moreover, the country came under criticism due to its deploying surveillance tools against dissidents and journalists-for instance, using Pegasus spyware-and was also

criticized over a highly publicized case concerning the journalist Jamal Khashoggi. These activities outline its dual role, both as a target and a user of cyber-capabilities, within the wider espionage landscape.

United Arab Emirates (UAE)

The UAE has risen as a regional leader in the sphere of cybersecurity, developing a mature infrastructure via NESA and partnering with large international tech firms. On the other side, it is accused of using the Pegasus spyware to perform political espionage, even including hacking operations during the Gulf blockade. Reliance on foreign partnerships for cyber tools indicates how modern technology in general is used in the country in a strategic way. The proactive stance of the UAE in both cyber defense and espionage underlines its role as a serious player in the evolving cybersecurity dynamics in the Arab world.

Qatar

The State of Qatar is a leader in the petroleum industry, one of the most prominent industries in the global stage. This quality makes it an extremely consequential actor in the politics of the Middle East, considering it has become a major economic hub because of its petroleum rich resources and technological development. The economic power that it holds makes it an increasingly important counterpart of the Middle East, opening it to major menaces from other nations. With technology being advanced in the country, cybersecurity and cyber espionage have emerged as the industrialization of the Arab States grew. These qualities along with its financial resistance puts the country in the midst of the proxy wars in the region, forcing it to invest in cyber security and espionage.

Chronology of Important Events

Date	*Description of Event*
24 January 2001	Arab Convention on Combating Information

	Technology Offences
21 November 2003	UN General Assembly Resolution 58/199 on the establishment of norms for the use of information and communication technologies
16 November 2005	World Summit on the Information Society (WSIS) Tunis Agenda
12 June 2010	Stuxnet Cyberattack
9 December 2012	UN Group of Governmental Experts (GGE) Report on Developments in the Field of Information and Telecommunications
18 December 2013	United Nations General Assembly Resolution 68/167 on Cybersecurity
25 September 2014	UN High-Level Event on Cybersecurity and Cybercrime
28 September 2015	UN General Assembly Resolution 70/237 on International Cybersecurity

6 November 2016	Establishment of the European Union Agency for Cybersecurity (ENISA)
9 December 2017	UN Secretary-General's High-Level Panel on Digital Cooperation
29 March 2018	Saudi Aramco Cyber Attack (Shamoon 2.0)
23 July 2018	United States indictment of Russian military officers for hacking and espionage during the 2016 U.S. elections
25 September 2018	United Nations Resolution on Digital Cooperation and International Law (73/215)
24 March 2021	European Union sanctions imposed on Russian entities and individuals involved in cyberattacks and espionage activities
11 June 2021	NATO's Cybersecurity Strategy 2021-2025 published, highlighting state-sponsored cyber threats

09 November 2022	Launch of the Global Forum on Cybersecurity Cooperation by the UN to address state-sponsored cyber activities

Relevant International Documents

- Resolution on Developments in the Field of Information and Telecommunications in the Context of International Security, 4 December 2018 (A/RES/73/27)
- Resolution on Combating the Criminal Misuse of Information Technologies, 16 January 2001 (A/RES/55/63)
- The Budapest Convention on Cybercrime, 23 November 2001
- The Arab Convention on Combating Information Technology Offences, 21 December 2010
- Resolution on Strengthening International Cooperation to Combat Cybercrime, 18 December 2019 (A/RES/74/247)
- Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013
- Resolution on the Creation of a Global Culture of Cybersecurity, 31 January 2003 (A/RES/57/239)
- Resolution on the Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, 30 January 2004 (A/RES/58/199)
- Resolution on Countering the Use of Information and Communications Technologies for Criminal Purposes, 27 December 2019 (A/RES/74/247)
- Programme of Action to Advance Responsible State Behaviour in the Use of ICTs in the Context of International Security, 2022 (A/RES/77/37)
- UN Guidelines for the Development of National Cybersecurity Strategies, 25 May 2016
- ITU Global Cybersecurity Agenda, 17 May 2007

- GGE Reports on Developments in the Field of Information and Telecommunications in the Context of International Security, 2010, 2013, 2015 (A/65/201; A/68/98; A/70/174)
- Arab Declaration on Cybersecurity, 28 March 2018
- Shanghai Cooperation Organisation Agreement on Cooperation in the Field of International Information Security, 16 June 2009
- ASEAN Cybersecurity Cooperation Strategy, November 2017
- The UN Draft Convention on Cybercrime, August 2024
- African Union Convention on Cyber Security and Personal Data Protection, 27 June 2014
- Resolution on the Use of ICTs for Sustainable Development, 12 July 2017 (A/RES/71/243)
- Resolution on Protecting Critical Infrastructure Against Cyber Threats, 23 February 2017 (A/HRC/RES/34/7)
- OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of ICTs, 2016
- EU Cybersecurity Strategy for the Digital Decade, 16 December 2020
- NATO Policy on Cyber Defence, 5 July 2011
- UNODC Comprehensive Study on Cybercrime, February 2013
- OECD Guidelines for the Security of Information Systems and Networks, 25 September 2002
- BRICS Declaration on Strengthening Cybersecurity Cooperation, September 2017
- G20 Leaders' Statement on Cybersecurity, 9 July 2017
- Resolution on Promoting the Right to Privacy in the Digital Age, 18 December 2013 (A/RES/68/167)
- UN Special Rapporteur Reports on Privacy in the Digital Age, 2015-2021
- Resolution on the Role of Science and Technology in the Context of International
- Security and Disarmament, 11 December 2018 (A/RES/73/32)

Past Attempts to Resolve the Issue

Multiple International, regional, and national attempts have been made by the Arab states in combating cyber espionage, but these actions that have taken place are limited. At least globally, a few organizations such as the United Nations Group of Governmental Experts have tried to develop a set of non-binding norms for responsible behavior in cyberspace, asking states to refrain from damaging each other's critical infrastructure through hacks. Similarly, the Paris Call for Trust and Security in Cyberspace has also tried to develop international cooperation in protecting digital systems. However, participation is spotty, and these initiatives lack rulemaking authority and punishment for violations.
The GCC has also drafted a strategy aimed at enhancing cybersecurity within its borders. For example, the GCC Cybersecurity Strategy 2021–2025 was initiated to enhance defenses, foster collaboration, and deal with common threats. However, these plans have rarely seen effective implementation due to political divisions-for instance, the blockade against Qatar in 2017-undermined trust and cooperation.

Countries like Saudi Arabia and the UAE have, at a national level, invested in Cybersecurity infrastructures: Kingdom of Saudi Arabia in 2017 established NCA with the view to protecting critical systems, and the UAE established NESA to focus on similar goals. The aim is to protect government networks, financial systems, and key industries against cyberattacks. These steps, however, tend to be essentially inward-looking with more emphasis on internal opposition surveillance than countering external threats of cyber espionage by world powers.

Notwithstanding these efforts, several challenges remain. Many Arab states depend on foreign technology and expertise in the area of cybersecurity-what might well introduce vulnerabilities. Political competition in the region also prohibits cooperation, while the lack of transparency works against trust and, ergo, information-sharing. Moreover, the partial application of cyber norms at the international level allows powerful states to get away from sanctions and proceed with espionage activities. These defects indicate that broader, more integrated, and stronger approaches are necessary to combat cyber espionage in the Arab world.

Regional members have been unable to enforce or adopt the Arab Convention on Combating Information Technology Offences due to inconsistencies within individual member states. The Same goes for cybercrime. Internationally bilateral efforts were made such as those made by the United Nations through the Group Experts on Development of International and Telecommunications Code to develop voluntary commitments and norms against state sponsored cyber activities. However, this faced pushback against countries that valued sovereignty over an international framework. Arab nations on the other hand have attempted to combat the issue on a national level through legislation aimed at establishing basic computer response task forces. But still faced the issues of limited resources, patchy tech development and a minimal focus on regional collaboration to make the cyber taskforce. Even now making a basic regional framework has proven to be a challenging task due to the ongoing political tensions along with a deep distrust between the Arab nations resulting in further deep fragmentation making responses against the increased cyber security issues more ineffective.

Solution Alternatives

Cyber espionage has to be duly met with a multidimensional response against internal vulnerabilities and external threats in the Arab region. A specifically created regional cybersecurity alliance, independent of existing political organizations, can bring the Arab states together to share intelligence, build capacity, and collective defense mechanisms; an unbiased framework ensures that there is mitigation of political rivalries. Public-private partnerships with global tech giants and local startups would bring innovative solutions to improve the defenses while not compromising sovereignty over sensitive data. A shift from offensive to defensive cyber strategies-including investments in advanced encryption, AI-driven threat detection, and protection of critical infrastructure-is what will provide resilience in the case of cyberattacks. The Arab states can also utilize their strategic position in the global energy and trade markets as a lever to exert diplomatic pressure on these powers that practice cyber espionage by using economic carrots and sticks. Public education campaigns to raise the level of cybersecurity literacy among citizens and businesses would

be empowered to identify and mitigate cyber threats, reducing risks like social engineering attacks. By adopting these measures in a coordinated and cooperative manner, the sovereignty of Arab states will be enhanced by protecting their digital infrastructure and building up a more secure and resilient cyber ecosystem for the future. Taking into account the broader context, the issue of blocking cyber espionage sponsored by states in Arab countries can be tackled using a combination of methods. The creation of a regional cybersecurity partnership would enable Arab countries to work together in sharing intelligence on threats, setting standards, and coordinating response to attacks. Such an initiative may draw lessons from the Cooperative Cyber Defence Centre of Excellence established by NATO, but modified to address peculiarities of the region. Opening up cybersecurity laws among Arab countries is very important to close the gaps in legislation and guarantee identical punishments to perpetrators of cyber espionage from tougher laws guarding against information and privacy abuse. Measures to build confidence including detailing of one's cyberspace capabilities or regularly conducting joint field maneuvers are also likely to be helpful in building trust and reducing inter state tensions. At the same time, countries should allocate considerable resources towards improving their cyber security infrastructure, provision of advanced technology and making sure essential services are protected against virtual attacks. Launching joint public and private projects which would tap the expertise of top information technology companies and supporting regional cyber education would improve resilience further.

Useful Links

- https://www.bbc.com
- https://www.reuters.com
- https://www.aljazeera.com
- https://www.theguardian.com
- https://www.nytimes.com
- https://www.washingtonpost.com
- https://www.economist.com

- https://www.theatlantic.com
- https://foreignpolicy.com
- https://www.foreignaffairs.com
- https://news.un.org
- https://www.interpol.int
- https://www.cfr.org
- https://www.oecd.org
- https://ccdcoe.org
- https://www.enisa.europa.eu
- http://www.lasportal.org
- https://asean.org
- https://www.itu.int
- https://www.unodc.org
- https://www.worldbank.org
- https://www.cisa.gov
- https://www.technologyreview.com

Bibliography

Chudarova, Valeria. “The Evolution of Cyber Espionage in the Arab World since the Beginning of the Arab Spring.” *Justice for Journalists*, 13 Nov. 2023, jfj.fund/the-evolution-of-cyber-espionage-in-the-arab-world-since-the-beginning-of-the-arab-spring/. Accessed 14 Jan. 2025.

“Connect the Dots on State-Sponsored Cyber Incidents - Cyber Espionage by the United Arab Emirates (UAE).” *Council on Foreign Relations*, www.cfr.org/cyber-operations/cyber-espionage-united-arab-emirates-uae. Accessed 15 Jan. 2025.

Corera, Gordon. “Five Russian Hacks That Transformed US Cyber-Security.” *BBC News*, BBC, 18 Dec. 2020, www.bbc.com/news/technology-55368211. Accessed 14 Jan. 2025.

Countering State-Sponsored Cyber Economic Espionage ..., securitypolicylaw.syr.edu/wp-content/uploads/2015/06/Lotriont e_Countering_State_Sponsored_Cyber_Economic_Espionage.pdf. Accessed 14 Jan. 2025.

“Cyber Espionage.” *Obo*, www.oxfordbibliographies.com/display/document/obo-9780199796953/obo-9780199796953-0212.xml. Accessed 14 Jan. 2025.

“Cybersecurity and New Technologies | Office of Counter-Terrorism.” *United Nations*, www.un.org/counterterrorism/cybersecurity. Accessed 14 Jan. 2025.

Cyberterrorism: How Real Is the Threat? | United States Institute of Peace, www.usip.org/publications/2004/05/cyberterrorism-how-real-threat. Accessed 14 Jan. 2025.

“Cyberwar.” *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., www.britannica.com/topic/cyberwar. Accessed 14 Jan. 2025.

Cyberwars in the Middle East, www.jstor.org/stable/48733389. Accessed 14 Jan. 2025.

“Espionage.” *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 22 Nov. 2024, www.britannica.com/topic/espionage. Accessed 14 Jan. 2025.

“How BAE Sold Cyber-Surveillance Tools to Arab States.” *BBC News*, BBC, 14 June 2017, www.bbc.com/news/world-middle-east-40276568. Accessed 14 Jan. 2025.

“Iran-Based Cyber Actors Enabling Ransomware Attacks on US Organizations: CISA.”

Cybersecurity and Infrastructure Security Agency CISA, 16 Oct. 2024, www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a. Accessed 14 Jan. 2025.

"IRGC-Affiliated Cyber Actors Exploit PLCS in Multiple Sectors, Including US Water and Wastewater Systems Facilities: CISA." *Cybersecurity and Infrastructure Security Agency CISA*, 16 Oct. 2024, www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a. Accessed 14 Jan. 2025.

Olech, Dr Aleksander. "Cybersecurity in Saudi Arabia." *Institute of New Europe*, 25 Mar. 2023, ine.org.pl/en/cybersecurity-in-saudi-arabia/. Accessed 15 Jan. 2025.

"Russia-Aligned Hackers Target European and Iranian Embassies in New Espionage Campaign." *Cyber Security News | The Record*, 17 Feb. 2024, therecord.media/russia-aligned-hackers-target-european-and-iranian-embassies-cyber-espionage. Accessed 14 Jan. 2025.

Schaer, Cathrin. "Why Is the Middle East Losing so Much Money to Cybercrime? – DW – 09/03/2024." *Dw.Com*, Deutsche Welle, 5 Sept. 2024, www.dw.com/en/why-is-the-middle-east-losing-so-much-money-to-cybercrime/a-70123520. Accessed 14 Jan. 2025.

"Significant Cyber Incidents: Strategic Technologies Program." *CSIS*, www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Accessed 14 Jan. 2025.

Special Report: Inside the UAE's Secret Hacking Team of U.S. Mercenaries | Reuters, www.reuters.com/article/world/special-report-inside-the-uaes-secret-hacking-team-of-us-mercenaries-idUSKCN1PO1CV/. Accessed 14 Jan. 2025.

"Suspected Iranian Cyber-Espionage Campaign Targets Middle East Aerospace,

Defense Industries." *Cyber Security News | The Record*, 28 Feb. 2024, therecord.media/iran-cyber-espionage-campaign-targeting-middle-east-defense-aerospace. Accessed 15 Jan. 2025.

"Tracking State-Sponsored Cyberattacks around the World." *Council on Foreign Relations*, www.cfr.org/cyber-operations/. Accessed 14 Jan. 2025.

Turkish Intelligence Dismantles Global Cyber Espionage ..., www.arabnews.com/node/2567224/middle-east. Accessed 14 Jan. 2025.

U.S. Department of State, www.state.gov/bureau-of-counterterrorism/executive-order-13224. Accessed 14 Jan. 2025.

U.S. Department of State, www.state.gov/u-s-takes-action-to-further-disrupt-russian-cyber-activities/. Accessed 14 Jan. 2025.

The United Nations, Cyberspace and International Peace ..., unidir.org/files/publication/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf. Accessed 14 Jan. 2025.

US Indicts Russian Intelligence Officials over Cyberattacks Targeting Ukraine | Reuters, www.reuters.com/world/us-indicts-russian-intelligence-officials-over-cyber-attack-targeting-ukraine-2024-09-05/. Accessed 14 Jan. 2025.

Zurier, Steve. "New Cyber Campaign Targeted Middle Eastern Government, Researchers Say." *SC Media*, 8 Oct. 2024, www.scworld.com/news/unspecified-middle-eastern-country-allegedly-targeted-by-new-cyber

-campaign-linked-to-iranian-backed-threat-group. Accessed 15 Jan. 2025.