Article

Not peer-reviewed version

Cybersecurity Challenges and the Protection of the Arabic Language in the Age of Artificial Intelligence: Digital Security and Safeguarding Methods

Driss Abbadi * and Abdelkader Lachkar

Posted Date: 10 March 2025

doi: 10.20944/preprints202503.0609.v1

Keywords: cyber threats; protecting the Arabic language; digital security; digital space; protection strategies; security technologies

 doi:10.20944/preprints202503.0609.v1

Article

Cybersecurity Challenges and the Protection of the Arabic Language in the Age of Artificial Intelligence: Digital Security and Safeguarding Methods

Driss Abbadi * and Abdelkader Lachkar

Public Law, Politics, Economics and Management Laboratory, Faculty of Polydisciplinary Studies, Taza, Sidi Mohamed Ben Abdellah University of Fès, Morocco

* Correspondence: driss.abbadi@usmba.ac.ma

Abstract: The Arabic language faces significant challenges in the digital age, particularly in the era of artificial intelligence, due to the increasing cyber threats such as digital attacks, data breaches, content manipulation, and data leakage. As the world experiences a rapid expansion in internet dependence across various fields such as education, media, and social communication, the Arabic language is exposed to risks that threaten its existence and continuity in the digital space. Protecting Arabic content from these threats requires special attention, through the implementation of effective security strategies, including modern encryption techniques and the development of tools to safeguard content from piracy. Additionally, raising public awareness about the importance of preserving the Arabic language in the age of artificial intelligence is essential. Governments, universities, and tech companies must collaborate to create secure digital environments that ensure the continuity of the Arabic language. The central issue addressed in this article is how to protect the Arabic language from cyber threats in the age of artificial intelligence and their negative impact on its sustainability in the digital space. **Research Objectives:** This research aims to examine the impact of cyber threats in the era of artificial intelligence on the Arabic language in the digital space. It analyzes various types of cyberattacks and content manipulation, exploring how these threats affect the continuity of the Arabic language and protect it from alteration or destruction. The study also seeks to present effective strategies and solutions for safeguarding the Arabic language from digital risks, including the development of digital protection tools and the enhancement of security policies. Additionally, the research emphasizes the importance of raising public awareness about preserving the Arabic language in the digital age by highlighting the growing risks it faces. **Methodology: -Descriptive Method**: Focuses on describing the challenges faced by the Arabic language in the cyber space, analyzing the patterns and trends affecting its use in the digital environment.**-Analytical Method**: Used to analyze the impact of cyber threats on the Arabic language in the digital space, studying the effects of cyberattacks and content manipulation on linguistic and cultural identity. **Key Findings:** -Cyber threats significantly affect the continuity of the Arabic language in the digital space, potentially leading to the destruction or distortion of Arabic content; -Content manipulation contributes to spreading inaccurate information, putting linguistic and cultural concepts at risk;-There is an urgent need to develop effective security strategies to protect the Arabic language from these threats; -Raising awareness in Arab communities about the importance of preserving the Arabic language in the digital space is a priority for its protection. **Key Recommendations:** -Develop effective digital protection tools, such as modern encryption techniques, to safeguard Arabic content; -Enhance collaboration between governments, academic communities, and tech companies to create secure digital environments; -Improve digital security policies to protect the Arabic language from cyberattacks; -Raise public awareness about the importance of protecting the linguistic and cultural identity of the Arabic language in the digital age; -Adopt educational strategies to inform individuals about the risks of cyber threats and how to interact with them safely.

 doi:10.20944/preprints202503.0609.v1

Keywords: cyber threats; protecting the Arabic language; digital security; digital space; protection strategies; security technologies

1. Introduction

Language holds a significant place in the Quran, as the word 'tongue' is mentioned in verse 4 of Surah Ibrahim and verse 22 of Surah Ar-Rum, referring to the diversity of languages among humanity, which were conveyed through the prophets. The Arabic language, in particular, occupies a prominent position, as it is the medium through which the Quran was revealed. This is highlighted in verses 13 and 33 of Surah An-Nahl, verse 195 of Surah Ash-Shu'ara, and verse 12 of Surah Al-Ahqaf (Jawhar, N.E., 2017).

Arabic is the core of our cultural and national identity; it is the bond that unites the members of our nation and brings them together. It also serves as the guardian of our heritage and Islamic identity (Kanaan, A. A, 2012, p.3). The Quran highlights the importance of this language, as Allah says: *'Indeed, We have sent it down as an Arabic Quran that you might understand'* (Yusuf: 2). Arabic was chosen to be the language of the Quranic verses, which convey precise and clear meanings. Furthermore, it is a language known for its remarkable ability to express a wide range of thoughts and emotions and is among the most capable languages in conveying profound meanings.

Allah Almighty has made the Quran clear and in Arabic, as He says: *'Alif Lam Ra. This is a book whose verses are perfected, then detailed from one wise and informed'* (Hud: 1). This language reflects everything in the human soul—its hopes and dreams. It serves as the primary means that connects members of society and expresses their joys and sorrows.

As the poet "Halim Demos" said:

A language, when it reaches our ears,
Is like a breeze soothing our hearts.
It will remain a bond that unites us,
For it is the hope of those who speak Arabic.

However, the Arabic language faces significant challenges in the context of globalization and Western cultural dominance. Many experts warn that the marginalization of the Arabic language could lead to the loss of a significant part of the cultural and intellectual identity of Arab nations (Ahmed, K. 2010, pp.196-200). These challenges are exacerbated in the digital age, with the rise of cyber threats such as breaches, content manipulation, and data leakage, alongside the widespread use of the internet in fields like education, media, and social media (Etuh, E., et al,. 2022). Therefore, the exposure of the Arabic language to risks that threaten its continuity in the digital space requires special attention and protection through effective security strategies, such as encryption techniques and raising public awareness about the importance of preserving it.

1.1. Importance of the Topic

In the current digital age, the era of artificial intelligence dominance, the Arabic language faces numerous challenges resulting from rapid technological advancements and the increasing reliance on the internet in various fields such as education, media, and social communication. These challenges include cyberattacks such as digital breaches, content manipulation, and data leakage, which could threaten the digital identity of the Arabic language. It is crucial to protect the Arabic language from these threats to ensure its continuity in the digital era and enhance its position among other global languages. Preserving the Arabic language is not only a cultural matter but also a fundamental pillar in safeguarding Arab identity in the face of rapidly advancing technological openness. This requires effective and well-thought-out strategies to protect Arabic content online, including the use of modern technologies such as artificial intelligence to ensure digital security.

1.2. Theoretical Level

 doi:10.20944/preprints202503.0609.v1

At the theoretical level, the cyber threats facing the Arabic language in the digital space are analyzed. These threats range from cyberattacks targeting Arabic content, such as text manipulation or data theft, to challenges arising from the spread of fake news or digital impersonation. Artificial intelligence can play a key role in countering these threats by applying advanced techniques such as suspicious pattern recognition, content manipulation detection systems, and big data analysis to identify any type of threat. Moreover, digital security is a central topic in this context, where advanced encryption techniques and content protection systems must be used to maintain the integrity of the Arabic language. In this regard, AI can offer innovative solutions that make the protection process more efficient and precise.

1.3. Practical Level

At the practical level, there are various ways to implement solutions to address cyber challenges and protect the Arabic language in the digital age. One such solution is the use of artificial intelligence for early detection of content manipulation or breaches that may occur to the Arabic language online. For example, intelligent systems can be developed to analyze texts and detect any illegal alterations or threats to Arabic content. Additionally, AI can assist in developing advanced encryption techniques to protect Arabic data and digital content from piracy. Practically, secure digital platforms can be created to store and share Arabic content safely, protecting it from digital risks. Furthermore, there must be collaboration between governments, universities, and tech companies to develop and implement effective security policies that safeguard the Arabic language in the digital space, by promoting initiatives that enhance digital security and raise user awareness.

1.4. Literature Review

1.4.1.Teaching Arabic in the Age of the Fourth Industrial Revolution Based on Quranic Guidelines

"Teaching Arabic in the Age of the Fourth Industrial Revolution Based on Quranic Guidelines" by Jawhar, Nasruddin Idris. The main goal of this article appears to be achieving a balance between Quranic guidelines and the latest methods from the Fourth Industrial Revolution in teaching the Arabic language, especially to non-native speakers. The article reviews several foundational elements supporting the development of Arabic language education and focuses on the importance of using modern technology such as the internet, digital media, and advanced technological tools in Arabic language instruction.

At the same time, it emphasizes the crucial role of educational objectives and content that should focus on the language skills required in the digital age. The article delves into adopting a comprehensive vision that includes using these technological tools to enhance education while preserving the essence of the Arabic language as part of cultural and religious identity, based on Quranic guidelines. As mentioned in the text, the Quran laid many foundations for learning language, making the study of Arabic not only a linguistic task but also a communicative and cultural one. From this perspective, the article highlights the importance of integrating technological tools with traditional educational strategies to create an effective and rich learning environment. It also underscores the multidimensional role that teachers must play in the age of the Fourth Industrial Revolution to meet the contemporary needs of students efficiently and effectively.

1.4.2. The Arabic Language and Contemporary Challenges and Ways to Address Them

"The Arabic Language and Contemporary Challenges and Ways to Address Them" by Kanaan, Ahmad Ali. This article discusses the challenges facing the Arabic language in the 21st century, highlighting the effects of globalization and the competition of the English language, which threaten Arab national identity. It also addresses the decline in the use of Modern Standard Arabic among Arabs due to the influence of local dialects. The study explores the phenomenon of the widespread use of local dialects, which have started to replace Modern Standard Arabic in many aspects of daily life. The researcher proposes several solutions to address these challenges, such as restoring

 doi:10.20944/preprints202503.0609.v1

confidence in the Arabic language and instilling a love for it in the new generations, keeping pace with technological developments by using modern technical tools in language teaching, and strengthening its position in society as a scientific and media language. The article calls for the development of educational curricula and language teaching methods to suit the present age, emphasizing the need for cooperation between families, schools, and the media to enhance the Arabic language's status and protect it from external influences.

1.4.3. The study titled "Cybersecurity Threats in the Age of Artificial Intelligence: Leveraging Advanced Technologies and Strengthening Cybersecurity"

The study titled "Cybersecurity Threats in the Age of Artificial Intelligence: Leveraging Advanced Technologies and Strengthening Cybersecurity" by driss Abbadi and Abdelkader Lachkar, published in October 2024 in the International Journal of Sciences and Research Archives, is a comprehensive analytical study exploring the interrelationship between artificial intelligence (AI) and cybersecurity threats in the modern digital era. The study examines how AI is being used to develop advanced cyberattacks and its role in enhancing cybersecurity systems to protect digital infrastructures from these growing threats.

The study begins by highlighting the rapid technological advancements in AI, which have opened new opportunities for cyber attackers to exploit these advanced technologies in carrying out complex and intelligent attacks. With AI, malicious software capable of adapting to the changing digital environment can be developed, making it harder to detect or stop. AI-driven attacks can learn from their interactions with targeted systems, enhancing their effectiveness and ability to evade traditional defense mechanisms.

In contrast, the study reviews AI's role in strengthening cybersecurity through techniques like machine learning and behavioral pattern analysis for early threat detection. By integrating AI into defense systems, the response to cyberattacks can be improved, enabling institutions to accurately analyze suspicious activities and respond rapidly to potential risks. The study also highlights AI's role in predicting future attacks and improving protection strategies based on big data.

One of the core points discussed in the study is the challenges cybersecurity faces in light of the continuous development of AI technologies. While AI helps enhance security defenses, it can also be exploited by attackers to develop advanced attack tools that could bypass traditional security barriers. The study emphasizes the need for a balanced strategy that integrates AI as an effective defensive tool against cyber threats while also staying ahead of emerging threats that AI might create.

Additionally, the study employs both descriptive and analytical methods to examine evolving patterns and attacks, using inductive reasoning to infer relationships between AI and information security. The study recommends strengthening cooperation between government entities and the private sector to combat advanced threats and continuous development of AI technologies to ensure effective cybersecurity responses. It also stresses the importance of training programs for specialists in this field to equip them to handle the security challenges arising from the use of AI.

This study serves as a call for urgent collaboration from all relevant parties to develop advanced defense strategies that keep pace with AI developments in all areas of cyber-attack and defense. While modern technologies offer significant opportunities to enhance the security of digital systems, they simultaneously present new challenges that require innovative and comprehensive strategies to mitigate their risks.

1.4.4. The study titled "The Joint Efforts of Media and Linguistic Institutions in Preserving the Arabic Language"

The study titled "The Joint Efforts of Media and Linguistic Institutions in Preserving the Arabic Language" by Mohamed Aziz Abdelmaksoud, Reda Owis Hassan Serour, and Mukhamad Hadi Musolin, highlights the crucial role of both media and linguistic institutions in preserving and promoting the Arabic language in the modern era. The study emphasizes the significant importance of the Arabic language in maintaining the cultural identity of the Arab nation and calls for collective

 doi:10.20944/preprints202503.0609.v1

efforts between various concerned parties, including the media and educational institutions, to ensure the preservation and development of the language. The researchers in this study discuss several fundamental questions, such as: Does the Arabic language have priority in the present age? What role do media and linguistic institutions play in preserving it? How can these efforts be enhanced?

Through the analysis of the study, it becomes clear that the media plays a key role in highlighting the beauty of the Arabic language and introducing its advantages and features to the public. Additionally, educational institutions related to linguistics can support this mission by providing effective education and developing curricula that align with the requirements of the modern era, thereby contributing to the widespread use of the Arabic language in various fields. The study also addresses the importance of leveraging modern technology and media to improve Arabic language teaching methods and enhance their effectiveness, which requires boosting the linguistic qualifications of teachers through specialized workshops and conferences.

One of the main points discussed in the study is the necessity of cooperation between government and academic institutions to develop modern educational strategies that align with contemporary challenges. It also discusses the critical importance of revising curricula in Arabic schools and universities to ensure they keep pace with modern developments and achieve their goal of enhancing the status of Arabic in both academic and public spheres. Practically, the study recommends developing training programs for linguistic staff and launching global linguistic projects aimed at improving the Arabic language proficiency of learners.

In conclusion, the study provides several important recommendations, such as the need to renew Arabic language teaching methods to make them more effective in addressing contemporary challenges. Based on these recommendations, it can be concluded that preserving the Arabic language requires a collective effort from the media, educational institutions, and governments to create a comprehensive linguistic renaissance that ensures the continued influence of the Arabic language in the modern world.

1.4.5. The study published in the International Journal of Innovation, Creativity and Change in 2020, titled “Artificial Intelligence Development and Challenges (Arabic Language as a Model)”

The study published in the International Journal of Innovation, Creativity and Change in 2020, titled “Artificial Intelligence Development and Challenges (Arabic Language as a Model)” by Mohammed MuzaaL Khalatia and Tahseen Ali Hussein Al-Romany, aims to discuss the development and challenges of artificial intelligence, using the Arabic language as a model. The study points out that Arabic content on the internet represents only 1% of the total content, despite the fact that Arabic speakers constitute 5% of the global population. This disparity reflects the significant gap between the number of Arabic speakers and the available content. The researchers attribute this gap to the lack of early awareness regarding the importance of machine translation (MT) and the scarcity of experts in this field.

The study addresses the definition of artificial intelligence (AI) and its ability to process data and make decisions similar to human thinking. It also highlights the role of Natural Language Processing (NLP), a branch of AI that analyzes human language using computers. The study elaborates on the challenges faced when using AI with the Arabic language, particularly due to the unique features of Arabic that distinguish it from other languages.

The study concludes with several recommendations to improve the use of AI in the Arabic language field. It stresses the need to develop techniques used in representing the semantic meaning of texts, especially through exploring deep learning techniques such as Word2Vec and InferSent. It also advocates for enhancing web browsers to improve their performance in Arabic language tasks and improving sentence representation. Additionally, the study emphasizes the importance of supporting linguistic technology to disseminate linguistic knowledge and make it more accessible to Arabic language users. The study also highlights the need to support linguistic planning by reforming the structure and phonetics of the Arabic language, as well as simplifying its writing rules.

 doi:10.20944/preprints202503.0609.v1

Furthermore, it sees it as crucial to support language policies by making decisive decisions regarding the relationship between language and science in the language acquisition process. Finally, the study underscores the importance of true collaboration between AI scientists and linguists to develop techniques that support the Arabic language in the context of modern technologies, thereby enhancing its use in various digital applications.

1.5. Research Problem

In today's world, digital technology and artificial intelligence have become an integral part of our daily lives. We are witnessing a rapid digital transformation across various sectors, including education, media, commerce, and many others. However, this technological advancement has not come without challenges, particularly for languages with limited digital presence, such as Arabic. Despite being one of the most spoken languages in the world, Arabic faces numerous challenges in the digital space, with one of the most prominent being cyber threats that could harm its presence and development in this domain.

The core issue of this research revolves around how to protect the Arabic language from contemporary cyber threats. With the widespread use of artificial intelligence, the risks to Arabic digital content are increasing, as cyberattacks could destroy or alter content in Arabic, reducing its presence on the internet and affecting its effectiveness on various digital platforms. Additionally, the challenges arising from competition with other languages, such as English, contribute to deepening this problem, as the digital dominance of other languages continues to grow.

Based on this reality, the research will address this issue through two main axes. The first axis will focus on studying the cyber threats and their impact on the Arabic language in the digital space, highlighting how these threats affect the online presence of Arabic and the AI tools used in this field. The second axis will be dedicated to strategies for protecting the Arabic language from these threats, focusing on possible technical solutions and necessary actions to strengthen the digital presence of Arabic and ensure its continued effective use in the face of rapid digital development.

1.6. From This Issue, the Following Research Questions Emerge

-What are the main types of cyber threats facing the Arabic language in the digital space?

-How do cyberattacks affect Arabic digital content and its presence on the internet?

-What are the effective digital tools available to protect the Arabic language from cyber threats?

-How can security policies be developed and awareness enhanced to maintain the security of the Arabic language in the digital space?

1.7. Main Hypothesis of the Research

The main hypothesis of this research is that contemporary cyber threats, in the era of artificial intelligence, pose a real threat to the existence of the Arabic language in the digital space. The hypothesis further assumes that the protection of the Arabic language from these threats can be enhanced through the development of effective strategies and technologies that ensure its continuity and development in the online environment.

This hypothesis is based on the belief that rapid technological advancement, particularly in the fields of artificial intelligence, may increase the exposure of the Arabic language to cyber risks, such as attempts to destroy or distort Arabic digital content or replace it with more dominant languages. At the same time, the hypothesis asserts that enhancing the presence and protection of the Arabic language requires a combination of technical and strategic efforts, including the development of digital protection tools tailored for the Arabic language, as well as fostering collaboration between institutions concerned with the Arabic language and technology experts, to ensure its continued use and development in the digital space.

1.8. The Conceptual and Theoretical Framework of the Research

 doi:10.20944/preprints202503.0609.v1

In order to address the issue raised in the article and test the main hypothesis, it is necessary to analyze and reconstruct the key concepts discussed in this article: **Arabic language, cyber challenges**, and **artificial intelligence**.

1.8.1. First Key Concept

"The Arabic Language**"**. The Arabic language is one of the oldest Semitic languages, which has continued to evolve and adapt through different periods. Arabic belongs to the Semitic language family, which also includes Hebrew and Aramaic. It has been the official language in the Arab region since ancient times. The Qur'an, which was written in Arabic, is one of the main factors that helped preserve the Arabic language and elevate its status, as the Qur'an became the reference for the language and the foundation of linguistic understanding for successive generations (Aboelezz, M., 2016, pp. 175-187).

The Arabic language is distinguished by significant diversity in its dialects, ranging from Modern Standard Arabic (MSA) to various colloquial dialects, which differ considerably from one country to another. This diversity reflects the vast cultural and geographical variations across the Arab world. Modern Standard Arabic has preserved its position as the language of religion, education, and culture. Although dialects have developed and are widely used in daily life, Modern Standard Arabic remains the official and literary language adopted in media, education, as well as in literature and the sciences (Auda, S., 2017)

Linguistically, Arabic is distinguished by its exceptional ability to derive and form complex structures, making it a language rich in meanings and connotations. Arabic relies on a complex morphological and phonetic system, reflecting its historical and cultural depth. It also has the ability to adapt to changes over time, whether by incorporating new vocabulary or through the influence of other languages during certain periods (Zaydan, J., 2017).

Historically, Arabic is one of the oldest and richest Semitic languages. It originated on the Arabian Peninsula and played a significant role in the development of human civilization throughout the ages. Arabic became the language of the Qur'an, which granted it a special sanctity and made it a medium for religious and scientific communication in the Islamic world. It contributed to the transmission and advancement of knowledge in various fields such as medicine, astronomy, and mathematics, significantly influencing the European Renaissance through Al-Andalus. Furthermore, Arabic has had an impact on many other languages, especially European languages like Spanish, which contains around 40% of its vocabulary with Arabic origins, and French, which includes about 500 Arabic words. Languages such as Persian, Urdu, and Turkish have also been influenced by Arabic, especially in religious, cultural, and economic terms. Thanks to its richness and flexibility, Arabic continues to symbolize cultural and civilizational identity today. Studies have shown that over 160 languages worldwide have been written in the Arabic script (Seif El-Islam, M., 2024).

Over time, especially in the modern era, new challenges have emerged for the Arabic language due to globalization and the spread of other languages, such as English. This has led to discussions about how to preserve the language's identity amidst modern influences. Despite these challenges, Arabic remains alive, as it is taught in schools, used in the media, and considered the language of science and literature in many countries (Aboelezz, M., 2016, pp. 175-187).

The Arabic language is not just a means of communication; it is an integral part of the identity and culture of the Arab people. It is the language of religion, science, and thought, with a long and rich history that reflects the cultural development of the Arab world (Aboelezz, M., 2016, pp. 175-187).

1.8.2. Second Key Concept

Cybersecurity challenges encompass a range of difficulties and threats associated with the increasing use of digital technology and the internet. According to the Naif Arab Academy for Security Sciences' glossary, this field includes terms related to various types of cybercrimes, digital evidence, and techniques linked to cyberspace. Among the most prominent of these challenges are

 doi:10.20944/preprints202503.0609.v1

security threats such as cyberattacks and malware, which target the theft of sensitive information, in addition to cybercrimes involving online criminal activities such as fraud and cyber extortion. The issue of privacy protection also emerges as a critical concern, as ensuring the confidentiality of personal information and safeguarding it from unauthorized use is paramount (Al-Murjan, A. R., et al. 2024). To address these challenges, international cooperation, along with the continuous development of security legislation and technologies, is essential.

To gain a deeper understanding of the concept of cybersecurity challenges, one can refer to a variety of specialized centers and websites that offer accurate and comprehensive information on this subject. Cybersecurity challenges are a set of risks and threats targeting digital systems and information networks, demanding significant attention from individuals, institutions, and governments. Among the most prominent sources is the National Cyber Security Centre (National Cyber Security Centre), which provides in-depth information on digital system threats, data protection, and the modern technologies used to combat cyberattacks (NCSC). The Cybersecurity and Infrastructure Security Agency (Cybersecurity and Infrastructure Security Agency) also offers comprehensive strategies to protect national infrastructure from cyberattacks, along with guidelines on how to handle digital threats (CISA). On the other hand, the Internet Corporation for Assigned Names and Numbers (ICAN, One World, One Internet) contributes to the protection of internet stability by addressing threats related to internet names and domains (ICANN). Furthermore, the Pew Research Center provides reports and studies highlighting the impacts of modern technology on society, including the cybersecurity challenges faced by individuals and communities, particularly in areas like privacy and digital security (Pew Research Center). The (Cyber Security Foundation - CSFPC™) offers advanced research and solutions for dealing with the growing digital threats, while the Cybersecurity Foundation focuses on raising awareness about the risks of cybersecurity challenges and provides educational resources to help individuals and businesses adapt to these risks. Through these sources, one can gain a comprehensive understanding of cybersecurity threats and the ways to confront them and protect digital systems from increasing attacks.

1.8.3. Third Key Concept

Artificial Intelligence: Artificial Intelligence (AI) is defined as computer programs designed to solve complex problems by performing operations similar to human cognition. This field is part of computer science, where intelligent systems and software are researched and developed. Research in this area was founded on the idea that a fundamental human trait—intelligence or human knowledge (Homo sapiens)—can be precisely defined so that a computer can simulate it. This raises numerous philosophical questions about the nature of reality and the behavior of artificial beings, issues that have been addressed and answered since ancient times through myths, literature, and intellectual theories. AI started with a highly optimistic concept but has undergone significant developments and notable changes over time (Singh, A. 2019, p.566).

The history of Artificial Intelligence (AI) spans several important stages, beginning in the early 1940s. Initially, in 1943, Warren McCulloch and Walter Pitts proposed a neural model based on artificial neurons, while Alan Turing introduced the Turing Test in 1950, which became the cornerstone for understanding AI. In 1956, the field of AI was established as an independent branch during the Dartmouth Workshop, organized by a group of scientists including John McCarthy and Marvin Minsky. In the following years, the field saw significant achievements, such as the development of programs like the "Logic Theorist" and "Knowledge-Based Systems." However, AI faced significant challenges during the 1960s and 1970s due to computational problems and difficulties in dealing with complex systems. In the 1970s, the focus shifted towards knowledge-based systems, such as the "DENDRAL" program, which utilized specialized knowledge to solve chemical problems (Russell, S. J., & Norvig, P. 2010, pp. 16-28).

These achievements and challenges have contributed to shaping Artificial Intelligence (AI) into what it is today, making it an essential part of the technology industry. AI has also become pivotal in solving many complex problems in the field of informatics. Among the key objectives that AI aims to

 doi:10.20944/preprints202503.0609.v1

achieve are: thinking, understanding, organizing, analyzing, communicating, vision, as well as the ability to manipulate and move objects. AI relies on a variety of tools and techniques, including search and analysis, intuition, probabilistic and economic methods, as well as other advanced approaches (Singh, A. 2019, p.566).

2. The First Axis: Cyber Threats and Their Impact on the Arabic Language in the Digital Space

The rapid development of information and communication technology has integrated our lives into the digital world, with the internet becoming an essential part of our daily lives, making us vulnerable to modern cyberattacks. As the use of this technology increases across all sectors, attackers are constantly searching for security vulnerabilities using advanced tools and techniques. They are even developing more complex and dangerous threats, exploiting weaknesses that may be invisible, allowing them to launch harmful attacks with a single mistake (Narwal, B., et al., 2019, pp.301-325). In this section, we will explore the various types of cyber threats and their impact on the Arabic language.

2.1. Types of Cyber Threats in the Digital Space

Cyber threats represent a significant challenge, not only to digital security but also to the Arabic language, making it increasingly difficult to maintain linguistic and cultural identity in the digital world (Alzahrani, I., et al., 2024, p.2526). These threats can be categorized into two main types: traditional cyber threats and AI-driven cyber threats (Abbadi, D., &Lachkar, A. 2024, p.2578).

2.1.1. Traditional Cyber Threats

These include attacks that existed before the rise of artificial intelligence and its widespread presence in the digital space. These threats typically rely on traditional techniques or relatively simple cyber tools. Examples of these attacks include:

2.1.1.1. Malware

It is usually classified into several categories based on how it enters the target system and the type of breach it aims to cause. There is the virus, a malicious software that spreads by copying itself into files that are transferred to the target, whether through email or by an unsuspecting human user. Worms, on the other hand, spread through the network between devices without the need for infected files. Then there is the Trojan horse, which is embedded in a program that appears to have a beneficial effect while hiding its malicious one. A logic bomb is triggered when a certain external event occurs, such as a specific date or time. A rabbit consumes certain system resources excessively, causing the system to crash. The backdoor allows an attacker to access the target system without going through the usual authentication procedures. Although there are specific classifications, some of these types may overlap, such as a virus containing a logic bomb function or a Trojan horse that includes a backdoor (Sharp, R. 2007, p.2).

2.1.1.2. Ransomware

A type of cyberattack that encrypts the user's data or restricts access to it, then demands a ransom to decrypt the data or restore access. These attacks have increased since 1989 and now often use digital currencies like Bitcoin to facilitate anonymous payments. There are three main types of ransomware: Ransomware-Crypto, which encrypts data; Ransomware-Locker, which restricts access to the device; and Ransomware-Sector MBR, which encrypts the master boot record without affecting the data. The level of threat varies depending on the encryption method and the approach used in the attack (Hoseini, A. 2022, pp.7-9).

2.1.1.3. Phishing

 doi:10.20944/preprints202503.0609.v1

Phishing is a social engineering attack used to steal user data, such as login credentials and credit card numbers. The attack typically involves sending an email that appears to be something the victim needs, prompting them to click on a link or download an attachment. The term "phishing" comes from the traditional concept of fishing, where the attacker uses bait to deceive the victim. The term first emerged in 1996 when hackers stole the passwords of America Online users. The attacks increased in 1998 through the use of message boards and newsgroups, and by 2000, they were carried out through mass emails. Phishing attacks target the theft of personal data, infecting devices with malware, stealing trade secrets, and exploiting security vulnerabilities (Bellusci, V., et al., n.d, pp. 1-5).

2.1.1.4. Denial of Service Attacks (DoS/DDoS)

Denial of Service (DoS) attacks have become a major threat to computer networks, targeting vital resources such as bandwidth, cache memory, or processing capacity, ultimately disrupting service performance. Initially, DoS attacks were used among attackers within clandestine circles, but with the development of tools, any average user can now execute these attacks. Currently, Distributed Denial of Service (DDoS) attacks have become more prevalent, as the attack is launched through a large network of distributed devices online, making the attack more complex and harder to defend against. The goal of a DDoS attack is to disrupt the target service by overwhelming it with an enormous amount of traffic, causing service outages or significant degradation (Gu, Q., & Liu, P, n.d, pp. 4-5).

These types of attacks can be carried out using traditional methods that rely on exploiting known security vulnerabilities or social engineering. However, cyberattacks have further evolved with the use of artificial intelligence.

2.1.2. Cyber Threats Driven by Artificial Intelligence

As artificial intelligence has advanced, new threats have emerged that leverage this cutting-edge technology. These types of attacks are characterized by the use of algorithms and advanced techniques, enabling attackers to continuously adapt and refine their strategies. Examples of such attacks include:

2.1.2.1. Adversarial Attacks in Artificial Intelligence

Adversarial attacks in AI rely on exploiting the vulnerabilities of AI models to manipulate the system into making incorrect decisions, disrupting security systems. These attacks involve subtly and carefully modifying input data so that it appears normal to humans but causes intelligent systems to fail. An example of this is altering images in a way that makes them unrecognizable by systems (Goodfellow, I. J., et al., 2015), such as facial recognition systems (Kurakin, A., et al., 2016). These attacks extend to various fields, such as transportation, where traffic signals can be subtly altered, leading to catastrophic decisions (Szegedy, C., et al., 2014). They also pose a threat in healthcare, where they could manipulate test results and diagnoses, putting patients at risk (Yuan, X., et al., 2019).

2.1.2.2. Artificial Intelligence in Malware

The use of artificial intelligence in malware has become a major challenge in cybersecurity, as these malicious programs can adapt to targeted systems and bypass traditional protection tools. Through techniques such as machine learning and deep learning, malware can analyze system behavior and identify vulnerabilities to exploit. Additionally, it can dynamically modify itself based on the environment of the targeted system (Saxe, J., & Berlin, K., 2018, pp.30-37). Big data analytics techniques are also used to identify the most effective attack strategies, increasing the malware's ability to evade security defenses (Anderson, H. S., et al., 2016).

2.1.2.3. Exploitation of Artificial Intelligence in Ransomware and Phishing Attacks

 doi:10.20944/preprints202503.0609.v1

Artificial intelligence is a key factor contributing to the evolution of cyberattacks such as phishing and ransomware, with attackers utilizing it to analyze personal data and target victims with convincing messages. Machine learning techniques make malware more capable of adapting to user behavior, making it harder to detect attacks (Begou, N., et al., 2024). In phishing attacks, AI is used to replicate voice and video in order to impersonate trusted individuals, enhancing the effectiveness of the attack. Attackers can also leverage AI to automate target searches and craft precise phishing messages, increasing the likelihood of the attacks infiltrating numerous victims (Abbadi, D., &Lachkar, A., 2024, p.2578). It can be noted that AI-driven phishing has become more targeted and personalized, as AI can gather and analyze data from multiple sources to determine the ideal times and locations for an attack (Aleroud, A., & Zhou, L., 2017, pp.160-196).

2.1.2.4. Manipulation of Digital Content (Deepfake)

In its narrow definition, 'deepfake' refers to a type of artificial content created using deep learning techniques, including the replacement of people's faces in videos. This type of content creates situations where individuals appear to perform actions or say words they never actually expressed. Additionally, there are other categories of deepfakes, such as 'coordinated mouth movement,' where mouth movements are synchronized with audio, and 'puppet master' techniques, which involve manipulating the target's facial expressions and eye movements to make it seem as though they are following someone else in front of the camera. These techniques are not limited to face-swapping but also include mouth and body movement manipulation, providing vast possibilities for altering AI-generated content (Aghava, M. S., et al., 2023, pp.64-65).

Most of these attacks, if not all, aim to alter or erase texts and data, including linguistic content such as written Arabic. These attacks pose a real threat to the continuity of the Arabic language in the digital space, as they could lead to distortion or complete loss of Arabic content. With the increasing use of the internet in education, media, and social communication, the Arabic language becomes vulnerable to these attacks, which could impact its accuracy and authenticity, putting it at risk of manipulation or destruction.

2.2. The Impact of Cyber Threats on the Arabic Language and Its Protection

Cyber threats targeting cultural identity, including the Arabic language as a prominent component of that identity, are on the rise. In the context of fifth-generation warfare, the Arabic language has become a target for cyber threats, with digital tools being exploited to destroy Arabic linguistic content and dismantle cultural ties between individuals. These attacks aim to reduce the connection between younger generations and their native language, leading to a decline in its usage in the digital space and fueling cultural and social divisions. According to recent studies, youth in some Arab countries are experiencing a decline in their connection to their language, due to the systematic promotion of foreign cultural influences by online platforms (El-Khoury, A. M., 2024).

Fifth-generation warfare aims to influence societal behavior and collective minds (Hasanaj, S., & Gurashi, R. 2023, p.1), with one of its targets being the Arabic language as a part of cultural identity. Through advanced techniques such as artificial intelligence and data analysis, public discourse can be distorted and directed, leading to the erosion of cultural and linguistic values. Misinformation in Arabic spreads rapidly online, with false information circulating faster than the truth and at much higher rates (El-Khoury, A. M., 2024).

In this regard, we provide a live example of cyber threats to the Arabic language: translation systems. Translation systems involve transferring the meaning of data and information from the original language to a target language. For example, a text in English is translated into Arabic for understanding by some recipients. Translation systems and applications have become widespread online, providing information to users in their native languages. However, due to the unique structure of the Arabic language and its specific set of symbols, it is extremely difficult to implement accurate translators. Therefore, the challenge lies in whether translation systems and applications

 doi:10.20944/preprints202503.0609.v1

deliver the correct meaning and information as intended in the original language (Noora Albalooshi et al. 2011, p.379).

With the advancement of Neural Machine Translation (NMT) systems, the output of machine translation has become more accurate, contributing to the widespread use of online translation tools and facilitating access to content in multiple languages, including Arabic. However, these systems face significant challenges, such as errors known as "machine hallucinations," where translations are grammatically correct but carry incorrect meanings, leading to a distorted understanding of the Arabic language. These errors can put Arabic texts at risk (Saadany, et.al., 2024), as cyberattacks may alter or destroy Arabic content, including deleting or modifying texts, directly impacting the cultural and linguistic identity of the Arab world. Moreover, manipulation of word meanings or their inflections can threaten the accuracy of available information.

This highlights the importance of protecting the Arabic language against digital threats by promoting its use in the digital space and developing technological strategies that support Arabic content and counter attempts to erase or marginalize it. These efforts are essential to raising linguistic and cultural awareness, reducing the impact of information warfare that threatens Arabic-speaking communities, and ensuring the preservation of linguistic identity while strengthening the presence of Arabic in the digital age (El-Khoury, A. M. 2024).

3. Second Axis: Strategies for Protecting the Arabic Language in Cyberspace

The issue of the Arabic language should not be taken lightly. Language, in general, is the "ultimate measure of human society," and according to John Stuart Mill, it is the "light of the mind"; the light that enables individuals to navigate and engage with all that culture encompasses. It is a key element in achieving cultural diversity (Ahmed, K., 2010). The Arabic language, in particular, has enjoyed widespread use for over a thousand years among various peoples, including Muslims, Christians, and Jews (Ernst, C. W., 2013). In order to restore its leading position, it is essential to adopt a precise and effective strategy to ensure its presence and protection in the digital world.

3.1. Digital Protection Tools for the Arabic Language

Digital protection tools are fundamental pillars for safeguarding the Arabic language in cyberspace. These tools include encryption systems and techniques to protect against hacking attacks. They help secure Arabic data and texts online, protecting Arabic content from manipulation or destruction through cyberattacks, thus preserving the Arabic linguistic and cultural identity.

3.1.1. Encryption Systems

David Kahn, one of the greatest historians in the field of cryptography, noted that the science of encryption originated in the Arab world. This fact was confirmed by some Arabic cryptographic treaties found in the Suleymaniye Library in Istanbul in 1980, as well as the works of other scholars who wrote about encryption and code analysis in the Arab world (Al-Omari, Ahmad H. 2018, p.164). This encryption, which is one of the most important tools for information protection in the digital age, should return to its original home—so to speak—where its foundations and development are centered. It is essential to make efforts to develop and improve encryption systems in a way that meets our cultural and technological needs, with the goal of creating a secure and sustainable environment for the Arabic language. This environment must be fortified against cyber threats that could distort or harm it, contributing to the preservation of the Arabic language's digital identity and protecting it from the increasing risks in the virtual world.

There must be openness to technologies such as advanced encryption and blockchain to protect the Arabic language in the digital space. Modern encryption techniques, such as asymmetric and symmetric encryption, help ensure data confidentiality and protect it from unauthorized access, which is vital for safeguarding Arabic content in digital systems. These technologies can be employed to secure textual data containing Arabic content, ensuring that this content is not tampered with or

 doi:10.20944/preprints202503.0609.v1

stolen, particularly in online applications such as websites or digital education systems(Abbadi, D., &Lachkar, A., 2024, p.2583).

As for blockchain technology, its potential lies in ensuring transparency and reliability in documenting Arabic texts and content online. For example, blockchain can be used to guarantee that Arabic digital content, such as e-books, news, articles, and cultural content, is not tampered with. By using blockchain, it is possible to ensure that Arabic texts published online remain unchanged and undistorted, preserving intellectual property rights and protecting Arabic cultural heritage (Tapscott, D., & Tapscott, A., 2016).

These technologies are part of future solutions to preserve the Arabic language against digital threats, helping to enhance the digital security of Arabic content.

3.1.2. Protection Techniques Against Arabic Language Breach Attacks

Cyber-attack response systems, artificial intelligence, and machine learning can be relied upon as advanced technologies to protect the Arabic language from cyber threats. These systems can contribute to securing Arabic digital content and safeguarding it from sophisticated attacks targeting textual data, digital applications, or knowledge content related to the Arabic language. Some examples include:

3.1.2.1. Automated Response to Attacks

These systems can detect potential threats related to Arabic content online, such as attempts to manipulate, distort, or plagiarize textual content (Paloalto, n.d.). Through artificial intelligence techniques, attempts to breach or attack content management systems containing Arabic texts can be identified, followed by immediate actions (Bassett, S., & Paquette, M. 2018) such as isolating the threats or correcting the data (Sharma, G., & Narayan, R. 2024, pp.1-19);

3.1.2.2. Data Analysis and Machine Learning

Machine learning techniques can be used to analyze large datasets containing Arabic content, enabling the early detection of suspicious or unusual patterns that may indicate cyber threats, such as attempts at manipulation or breaches. These systems can learn and adapt to new patterns of attacks that may target Arabic digital content (Abbadi, D., & Lachkar, A., 2024, pp.2583-2584);

3.1.2.3. Smart Security

Artificial intelligence can enhance the digital security of Arabic content, whether on applications, websites, or social media platforms, by quickly and efficiently detecting cyberattacks such as ransomware or attacks on unknown security vulnerabilities that could affect Arabic-language data (Abbadi, D., & Lachkar, A., 2024, pp.2583-2584);

3.1.2.4. Real-Time Protection

The key benefit of these systems is their ability to act in real time to confront threats, thereby helping protect systems that host Arabic content or provide services in Arabic, whether educational platforms, websites, or communication applications (Abbadi, D., & Lachkar, A., 2024, pp.2583-2584).

By integrating advanced encryption with these automated systems, it is possible to ensure that Arabic data is not breached or manipulated, thus enhancing security and maintaining the integrity of Arabic content in the digital space.

Of course, this also requires the establishment of strict legislation and policies to ensure the responsible use of these technologies, which contributes to protecting the Arabic language in cyberspace. These policies should include legal and procedural mechanisms to safeguard Arabic content from manipulation or digital threats and provide a secure environment to ensure the continuity and protection of the language from any attacks that could jeopardize its existence in the digital world.

 doi:10.20944/preprints202503.0609.v1

3.2. Developing Security Policies and Raising Awareness

Security policies are essential factors in ensuring the protection of the Arabic language in cyberspace. This requires the development of comprehensive strategies that include strengthening legislation to protect Arabic from cyber threats, as well as organizing community awareness campaigns about the importance of safeguarding the Arabic linguistic and cultural identity. Furthermore, it is crucial to enhance Arab collaboration to prevent attacks that target, distort, or destroy Arabic texts.

3.2.1. Strengthening Legislation to Protect the Arabic Language from Cyber Threats

If we look at the Model Arabic Language Law issued by the International Council for the Arabic Language and adopted by the Arab Parliament (International Council for the Arabic Language, 2022), we notice that it focuses on a range of important issues related to the Arabic language. However, it clearly overlooks the issue of cyber threats, which pose a significant risk to the language in the digital space. The risks facing the Arabic language in today's digital environment are not mere hypotheses, but real challenges that require a response through strict legislation aimed at protecting Arabic texts from manipulation or cyber destruction. Any law dedicated to the Arabic language must include mechanisms to safeguard it from these growing digital threats, ensuring its continued role as a vital means of communication and cultural exchange in the digital age.

3.2.2. Strengthening Arab Cooperation to Protect Arabic from Cyber Threats

Arab cooperation in combating cybercrimes is embodied in the Arab Convention on Combating Information Technology Crimes, which was signed on December 21, 2010, by 21 countries (Al-Bidri, A. W. 2021, pp.105-106). According to Article 1 of the Convention, the aim is to enhance cooperation among member states in addressing information technology crimes, which pose a threat to the security and interests of states, communities, and individuals (Radi, S. M. A., 2019, p.31).

This Convention consists of five main chapters and forty-three articles. Chapter 1 provides general provisions about the Convention, while Chapter 2 addresses criminalization and outlines the types of crimes related to the misuse of information technology. Chapter 3 deals with procedural provisions, and Chapter 4 focuses on legal and judicial cooperation among the signatory countries. The fifth and final chapter addresses the concluding provisions **(**This agreement was drafted in Arabic in Cairo, Arab Republic of Egypt, on 15/1/1432 AH, corresponding to 21/12/2010 AD. An original copy of the agreement was deposited with the General Secretariat of the League of Arab States (Technical Secretariat of the Council of Arab Ministers of Justice), and the General Secretariat of the Council of Arab Ministers of Interior received a certified copy. A certified copy was also provided to each of the contracting states. Consequently, their Excellencies, the Ministers of the Interior and Justice of the Arab states, signed this agreement on behalf of their countries**)**.

The Convention specifies its scope of application in four cases: when the crime is committed in more than one country, when the crime is planned or overseen from another country, when the crime is linked to an organized criminal group operating across countries, or when the crime has severe impacts on other countries (Radi, S. M. A., 2019, pp.31-32).

Additionally, ESCWA as part of the project 'Cyber Legislation Coordination to Stimulate the Knowledge Society in the Arab Region,' implemented between 2009-2012, prepared the 'ESCWA Cyber Legislation Guidelines,' which serve as legislative models for the countries of the region. These guidelines cover, in addition to cybercrimes, electronic communications, freedom of expression, electronic signatures, electronic transactions, e-commerce, consumer protection, the processing of personal data, and intellectual property rights in the informational and cyber domains (Al-Bidri, A. W. 2021, pp.105-106).

However, despite the efforts made to combat cybercrimes through the Arab Convention on Combating Cybercrime and the guidelines prepared by ESCWA, the protection of the Arabic language and its data in the digital space has not received sufficient attention. Therefore, there is a

 doi:10.20944/preprints202503.0609.v1

need to increase focus on safeguarding the Arabic language in cyberspace and to develop legislative policies that ensure the preservation and security of Arabic texts against digital threats.

4. Conclusions

It is evident that cyber threats pose a significant challenge to the preservation of the Arabic language in the digital space. Protecting the Arabic language requires comprehensive security strategies that include advanced technologies for data protection and content encryption, along with the activation of effective security policies and enhancing cooperation between governments, academics, and tech companies. Additionally, raising public awareness about the importance of protecting the Arabic language in the digital age is a fundamental step in preserving the linguistic and cultural identity of the Arab nation. Through collective and continuous efforts in this field, the sustainability of the Arabic language in cyberspace can be ensured, protecting it from increasing threats and thus safeguarding the cultural identity for future generations in the face of global digital transformations.

It is beneficial to highlight some key recommendations, including:

-Teachers should effectively engage with modern technological tools available in educational settings, such as utilizing linguistic instructors for teaching speaking skills and internet networks for teaching reading skills. Additionally, teachers should skillfully use reliable and safe online resources for students (Jawhar, N.E., 2017);

-Technologies for Text Representation: The technologies used for text representation, such as Word2Vec (In artificial intelligence and machine learning, Word2Vec is a set of models used for word representation (word embedding). These models were developed by a research team at Google under the supervision of Tomas Mikolov) and InferSent **(**InferSent is a sentence representation method that provides semantic representations for English sentences. It was trained on natural language inference data and generalizes well to many different tasks. Link: https://tinyurl.com/4p8t6ede**)**, must be further developed;

-Training Engines for Optimal Performance: Engines must be trained to achieve the best performance for tasks related to the Arabic language, particularly at the sentence level, utilizing appropriate linguistic techniques such as sentence structure, parts of speech, and the ability to identify extraneous sentences (MuzaaLKhalati, M., 2020,p.924);

-Support for Linguistic Technology: Linguistic technology should be supported to promote the dissemination and accessibility of Arabic knowledge among Arabic language users (MuzaaLKhalati, M., 2020,p.924);

-Development of the Arabic Language: The Arabic language should be developed through the reform of its structure, reduction of writing rules, and the protection and modernization of its vocabulary (MuzaaLKhalati, M., 2020,p.924);

-Collaboration between AI and Linguists: There should be collaboration between artificial intelligence researchers and linguists to improve the understanding and security of the Arabic language(MuzaaLKhalati, M., 2020, p.924);

-Cybersecurity Framework: The cybersecurity framework must include the protection of intellectual, cultural, and social Arab systems, establishing a foundation for preserving national identity and intellectual awareness. This requires building a national intellectual system based on collective awareness and resistance to external influences, ensuring the community can withstand challenges that threaten its security and stability. This starts with updating policies, educational curricula, strengthening the role of community institutions, and developing national content that supports intellectual and cultural security (Khouri, A. M., 2024);

-Innovative Approaches to Arabic Language Education: Officials in all institutions involved in teaching and learning Arabic should develop modern methods and strategies for teaching Arabic to native and non-native speakers, using internet technologies to secure the process. It is also essential to offer linguistic projects through digital platforms to enhance the learning experience for students worldwide. Furthermore, online training programs should be implemented to build qualified

 doi:10.20944/preprints202503.0609.v1

linguistic competencies and scientific staff capable of teaching Arabic in a way that combines both tradition and modernity. Online seminars, workshops, and conferences should be held with the participation of linguists and educators to equip teachers with the necessary skills and knowledge for effective and secure teaching in the digital age (Abdelmaksoud, M. A., et al, 2023);

-Training Programs for Cybersecurity: Incentive-based training programs and specialized courses should be organized to grant certifications to cybersecurity specialists, both at the national level and within various sectors. These programs should be part of efforts to protect the Arabic language in the digital space, working to develop technological tools and security measures to safeguard Arabic digital content from cyber threats. This can be achieved through collaboration with non-governmental organizations, various institutions, internet service providers, libraries, protected trade organizations, community centers, computer storage facilities, and secure communities. Furthermore, programs should be created to promote education for adults, schools, and civil society organizations, with the goal of raising awareness of the importance of protecting the Arabic language in the digital space and securing its content from hacking or distortion, thus ensuring comprehensive and effective benefits (Arshi, Gabriel. 2025, p.119).

References

1- Abbadi, D., &Lachkar, A. (2024). Cyber threats in the age of artificial intelligence: Exploiting advanced technologies and strengthening cybersecurity. *International Journal of Science and Research Archive, 13*(01), Retrieved from https://doi.org/10.30574/ijsra.2024.13.1.1961.

2- Abdelmaksoud, M. A., et al, (2023). Concerted efforts of the media and linguistic institutions in preserving the Arabic language. *International Journal of Academic Research in Business and Social Sciences, 13*(10). https://doi.org/10.6007/IJARBSS/v13-i10/18721.

3- Aboelezz, M. (2016). A history of the Arabic language and the origin of non-dominant varieties of Arabic. In R. Muhr, K. E. Fonyuy, Z. Ibrahim, & C. Miller (Eds.), *Pluricentric languages and non-dominant varieties worldwide Part I: Pluricentric languages across continents. Features and usage.* (pp. 175-187). Peter Lang. https://eprints.bbk.ac.uk/id/eprint/24993/.

4- Aghava, M. S., et al., (2023). AI deep fake detection research paper. *International Journal of Novel Research and Development (IJNRD)*, 8(10), (pp.64-65). https://tinyurl.com/3e4f9jfr

5- Ahmed, K. (2010). The Arabic language: Challenges in the modern world. *International Journal for Cross-Disciplinary Subjects in Education, 1*(3), (pp.196-200). https://doi.org/10.20533/ijcdse.2042.6364.2010.0027.

6- Al-Bidri, A. W. (2021). Cybersecurity strategy: A case study of Morocco. *Democratic Arab Center for Strategic*, Political, and Economic Studies, [Translated from Arabic].

7- Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, 68, (pp.160-196). https://doi.org/10.1016/j.cose.2017.04.006.

8- Al-Murjan, A. R., et al. (2024). Dictionary of Key Terms in Cybercrimes and Digital Evidence: English - Arabic. Naif University Publishing House.

9- Al-Omari, Ahmad H. (2018). ABJAD Arabic-Based Encryption.(Vol. 9, No. 10). Northern Border University, KSA: *International Journal of Advanced Computer Science and Applications(IJACSA)*,Retrieved from https://tinyurl.com/3bz8dvw9.

10- Alzahrani, I., et al., (2024). Enhancing cyber-threat intelligence in the Arab world: Leveraging IoC and MISP integration. *Electronics, 13*(13), (p.2526). https://doi.org/10.3390/electronics13132526.

11- Anderson, H. S., et al., (2016). DeepDGA: Adversarially-tuned domain generation and detection, In *Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security, Retrieved from:* https://doi.org/10.48550/arXiv.1610.01969.

12- Arshi, Gabriel. (2025). Information Security in the Arab World: Risks and Challenges. *International Journal of Informatics, Media, and Communication Technologies, 119.* https://doi.org/10.21608/ijimct.2019.66251.

13- Auda, S. (2017, July 23). Between colloquial and classical Arabic: Does diglossia pose a threat to the language?, *Al Jazeera*. [Translated from Arabic], https://tinyurl.com/nwe5uude.

14- Bassett, S., & Paquette, M. (2018). Improve Security Analytics with the Elastic Stack, Wazuh, and IDS. *Elastic Blog*. Retrieved from bit.ly/4gx6rpX.

 doi:10.20944/preprints202503.0609.v1

15- Begou, N., et al. (2024). Exploring the dark side of AI: Advanced phishing attack design and deployment using ChatGPT. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*. https://bit.ly/3ZBZ7mB.

16- Bellusci, V., et al., (n.d.). Phishing (Edition not mentioned). Université Côte d'Azur. (pp. 1-5), Retrieved from https://tinyurl.com/mtkb3cak.

17- Cybersecurity and Infrastructure Security Agency. (n.d.). *CISA logo*. Link: https://tinyurl.com/mr34385w.

18- Cyber Security Foundation - CSFPC™, link **:** https://tinyurl.com/2jtztvky.

19- El-Khoury, A. M. (2024). The silent battles in fifth-generation warfare. *Arab Union for Digital Economy*. (Translated from Arabic). https://tinyurl.com/mtennnvt.

20- Ernst, C. W. (2013). The global significance of Arabic language and literature. *Religion Compass*, 7(6), 191. https://doi.org/10.1111/rec3.12049.

21- Etuh, E., et al,. (2022). Social media networks attacks and their preventive mechanisms: A review. *arXiv:2201.03330 [cs.SI]*. https://doi.org/10.48550/arXiv.2201.03330.

22- Goodfellow, I. J., et al., (2015). Explaining and harnessing adversarial examples. *arXiv* preprint arXiv:1412.6572.

23- Gu, Q., & Liu, P. (n.d.). Denial of service attacks. *Texas State University – San Marcos; Pennsylvania State University*. Retrieved from https://tinyurl.com/3sna9cd5.

24- Hoseini, A. (2022). Ransomware and phishing cyberattacks: Analyzing the public's perception of these attacks in Sweden (Edition not mentioned). *Uppsala University*. https://tinyurl.com/bdmzw9y8.

25- ICAN, One World, One Internet, link: https://www.icann.org.

26- International Council for the Arabic Language. (2022). Model Arabic Language Law (2nd ed.). [Translated from Arabic], Retrieved from https://tinyurl.com/mr25h2rc.

27- Jawhar, N. E. (2017). Teaching Arabic in the era of the Fourth Industrial Revolution. based on Quranic guidelines [Translated from Arabic]. *Lisan Arabi*. Retrieved from https://tinyurl.com/2skksevp.

28- Kanaan, A. A. (2012). Arabic language and contemporary challenges and ways to address them [Translated from Arabic] (p. 3). Retrieved from https://tinyurl.com/f3csffwk.

29- Khouri, A. M. (2024). The silent battles in the fifth-generation wars. *Arab Union for Digital Economy*. Retrieved from https://tinyurl.com/mtennnvt.

30- Kurakin, A., et al., (2016). Adversarial examples in the physical world. *arXiv preprint arXiv*:1607.02533.

31- MuzaaLKhalati, M. (2020). Artificial intelligence development and challenges (Arabic language as a model). *International Journal of Innovation, Creativity and Change*, 13(5), 924. Retrieved from https://tinyurl.com/4jabez6v.

32- Narwal, B., et al., (2019). Towards a taxonomy of cyber threats against target applications. *Journal of Statistics and Management Systems*, (3), (pp.301-325). https://doi.org/10.1080/09720510.2019.1580907.

33- National Cyber Security Centre. Link : https://www.ncsc.gov.uk/.

34- Noora Albalooshi et al.(2011).The Challenges of Arabic Language Use on the Internet, *6th International Conference on Internet Technology and Secured Transactions*, (p. 379), Abu Dhabi, United Arab Emirates, Retreived from https://tinyurl.com/mr3v8xay.

35- Paloalto. (n.d.). What is security automation? Retrieved September 25, 2024, from https://bit.ly/3ZWFDJV.

36- Pew Research Center, link : https://www.pewresearch.org/

37- Radi, S. M. A., (2019). *Cybercrime and the integration of national, regional, and international texts*. Hassan II University Publications Series, (Issue 23). Morocco: Journal of Law and International Business, [Translated from Arabic].

38- Russell, S. J., & Norvig, P. (2010). Artificial intelligence: A modern approach (3rd ed). Pearson Education.

39- Saadany, Hadeel, Tantawy, Ashraf, Orăsan, Constantin. (2024). Cyber Risks of Machine Translation Critical Errors: Arabic Mental Health Tweets as a Case Study. Retrieved from https://arxiv.org/abs/2405.11668Saxe, J., & Berlin, K. (2018). Deep neural network based malware detection using two-dimensional binary program features. *Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW),* 13(2), (pp.30–37). https://doi.org/10.1109/SPW.2018.00017

41- Seif El-Islam, M., (2024, May 29). The Arabic language and keeping up with the times: Universality, survival, and modern technologies. *Center for Arab Unity Studies*. https://tinyurl.com/3sa27599

 doi:10.20944/preprints202503.0609.v1

42- Sharma, G., & Narayan, R. (2024). AI-Driven Cybersecurity: Enhancing System Resilience With Advance Security Automation Program (ASAP). *Journal of Open Source Developments*

43- Sharp, R. (2007). An introduction to malware (Edition not mentioned). https://tinyurl.com/mr37bxbs.Singh, A. (2019). The concept of artificial intelligence. *Journal of Emerging Technologies and Innovative Research (JETIR)*, 6(3), 566. https://tinyurl.com/3fh7mmya.

45- Szegedy, C., et al., (2014). Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199*.

46- Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind bitcoin is changing money, *business, and the world*. Penguin.

47- Yuan, X., et al., (2019). Adversarial examples: Attacks and defenses for deep learning. *IEEE transactions on neural networks and learning systems*, 30(9)

48- Zaydan, J. (2017). Tārīkh Ādāb al-Lughah al-'Arabīyah [A history of the literature of the Arabic language]. *Hindawi*. [Translated from Arabic]. https://tinyurl.com/4nm984cz