INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 15, Issue 6, (2025) E-ISSN: 2222-6990

Cybersecurity and Protection of Digital Data Privacy in the UAE in the Age of Digital Transformation and Artificial Intelligence

Maitha Musabah Salem Bin Dhawi Al Khateri, Diaya Ud Deen Deab Mahmoud Al Zitawi

Academy of Islamic Civilization, Faculty of Social and Islamic Sciences, Universiti Teknologi Malaysia, Malaysia

Email: musabahsalem@graduate.utm.my, diaya@utm.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v15-i6/25445 DOI:10.6007/IJARBSS/v15-i6/25445

Published Date: 16 June 2025

Abstract

Information security is one of the most pressing challenges in the era of the Fourth Industrial Revolution, as modern institutions heavily rely on the data they possess. However, network-connected systems are increasingly exposed to various forms of breaches, raising concerns about the readiness of the United Arab Emirates' electronic defense systems. This study aims to examine the current state of cybersecurity and data privacy in the UAE, and the significance of these issues within the country's national security framework. It explores the types of cyber threats facing the UAE, the modern technologies used in cyberattacks, and the main challenges hindering the implementation of internal security policies. Additionally, it investigates the preventive and responsive measures adopted to counter such attacks. The UAE's comprehensive digital transformation has amplified potential risks to its national security and critical infrastructure, particularly amid the rapid evolution of artificial intelligence technologies. Therefore, the study underscores the importance of this topic due to its direct implications for national security and the protection of personal data. Relying on a desk research methodology based on scholarly sources and official reports, the study reveals that the UAE has made significant strides in cybersecurity through the development of a national strategy, the establishment of the Telecommunications Regulatory Authority (TRA), and the enactment of cybercrime legislation. The findings indicate that the UAE possesses strong cyber defense capabilities supported by governmental coordination and international cooperation. Despite the growing complexity of cyber threats and the rapid pace of technological advancement, the study highlights the critical need for enhancing cyber awareness, continuous education, and specialized training to reinforce the country's cybersecurity posture.

Keywords: Cybersecurity, Digital Data Privacy, Cybercrime, Digital Transformation, Artificial Intelligence.

Introduction

There is no doubt that information security refers to a set of procedures and measures taken by institutions and individuals to protect their electronic systems, sensitive information, and data from electronic threats and cyberattacks. It aims to ensure the integrity and confidentiality of information, maintain the availability of digital services, and safeguard the digital infrastructure of organizations and institutions. Digital security, in this context, is a concept closely related to cyber or electronic security. However, it places a broader focus on the digital and electronic aspects of safety. It also includes a range of processes, policies, and practices that aim to preserve the security of the digital world. (Al-Muhairi, 2023)

The issue of information security and protection is considered one of the most pressing concerns of our time — the era of the Fourth Industrial Revolution — where the success of any organization greatly depends on the information it holds. However, many of these systems, networks, and infrastructures connected to the internet are constantly at risk, facing various types of data breaches and criminal activities (such as hackers) that disrupt their services and damage their assets. Hacker attacks vary depending on the source, location, and time, using ever-evolving tools and techniques. This reality underscores the importance of electronic security to maintain national and public safety. (Salem, 2022)

One of the key focus areas of cybersecurity efforts in the United Arab Emirates is improving the level of digital security and ensuring the sustainability of digital technologies and societal advancement. A national cybersecurity strategy has been developed with the aim of enhancing electronic security and protecting information and the country's digital infrastructure. (Al-Humaidi, 2023)

This strategy outlines specific objectives and guiding principles to promote cybersecurity across all sectors. It is reflected in initiatives such as the establishment of the Telecommunications Regulatory Authority (TRA), which plays a pivotal role in boosting cybersecurity in the UAE. The TRA is responsible for regulating and monitoring the telecommunications and information technology sector, as well as developing policies and regulations related to cybersecurity. In addition, the UAE has introduced a comprehensive set of laws and regulations to strengthen cybersecurity, including the Cybercrimes Law, the Data Protection Law, and other legislative frameworks designed to regulate and secure the cyber domain.

Within this framework, the vision of the United Arab Emirates (UAE) has aimed at comprehensive national development, including the economy, security, citizen well-being, and quality of life. Naturally, one of its key objectives has been the shift toward the digital world, ensuring its electronic protection and the development of a robust digital infrastructure. This reflects the country’s commitment to keeping pace with the rapid global progress in digital services, evolving global networks, information systems, and operational technologies. It aligns with the growing capabilities in data processing, massive data storage, and communication, all of which prepare the ground for harnessing artificial intelligence and the transformations of the Fourth Industrial Revolution. (Nassr, 2021)

The significance of studying cybersecurity stems from its position as one of the most pressing contemporary challenges in light of the rapid global digital transformation. This is especially

true in the context of the United Arab Emirates (UAE), where cybersecurity has evolved from being a mere technical luxury to becoming a strategic necessity. The increasing frequency and complexity of cyber threats pose substantial risks to critical infrastructure, government institutions, and sensitive economic sectors. As reliance on technology, artificial intelligence, and the Internet of Things continues to grow, there is an urgent need to assess the nation's readiness to safeguard its digital space and ensure the safety of its users.

This study acquires even greater relevance within the UAE context, given the country's advanced efforts to build a comprehensive digital society. These efforts underscore the need to secure the digital ecosystem. The research also sheds light on the strategies and policies adopted by the UAE to enhance its capacity to counter cyberattacks, thereby contributing to the evaluation and improvement of these policies in support of both national and economic security.

Furthermore, this study offers analytical insights that assist policymakers and researchers in gaining a deeper understanding of cybersecurity challenges and risks. Such insights enable the development of more efficient and proactive protection frameworks. Accordingly, the study of cybersecurity serves not only an academic or theoretical purpose but also has practical implications, contributing to the enhancement of cyber resilience and the establishment of a secure and sustainable digital environment.

Cybersecurity has become a dilemma of our time, regarded as a modern strategic weapon due to the technological reality that imposes itself on societies, bringing with it unknown cyber threats and unpredictable attacks that raise concerns globally. With the UAE accelerating its digital transformation across vital sectors and sensitive infrastructures, it has become essential to examine the nation’s commitment to securing its electronic systems and digital information infrastructure. The key issue lies in assessing the preparedness of the UAE’s cyber defense systems, which can be derived from the national strategies and mechanisms the country adopts to protect its critical information structures.

This topic gains further importance in light of the technological revolution, which has led to a surge in the number of devices connected to the internet — creating fertile ground for cybercrime. There is no doubt that digital and cybersecurity are crucial for national security, given their role in protecting various critical sectors from cyberattacks. The UAE is among the leading nations that have taken significant steps to enhance its cybersecurity practices, such as approving the National Cybersecurity Strategy and announcing the formation of a Cybersecurity Council. This council was established to bolster cybersecurity and raise the preparedness of all sectors to respond to cyber threats.

This study aims to define the concept of cybersecurity and highlight its importance in the current digital era. It also seeks to examine the UAE’s role in this field by shedding light on the efforts and initiatives undertaken to strengthen cybersecurity. Furthermore, the study aims to analyze the national strategies, mechanisms, regulations, and legislation designed to enhance cybersecurity in the UAE. It evaluates the readiness of electronic defense systems to counter cyber threats and highlights the challenges the UAE faces in the cybersecurity domain, as well as the opportunities that can be leveraged to improve the overall cybersecurity posture.

To achieve the objectives of this study, a comprehensive methodology will be adopted, involving desk research to collect information and data from books, scientific articles, and official reports related to cybersecurity and the role of the UAE in this field.

The Concept of Cybersecurity

The term cyber is derived from the Greek word Kybernets, which means "the one who steers the ship." Some trace the origin of the term to the mid-20th century with American mathematician Norbert Wiener's use of it to describe automated control. He defined cybernetics as "control and communication in animals and machines," and described it as the "science of transmitting messages between humans and machines or between machines themselves." From this, the concept of cybernetics evolved to express automated processes and the relationships between electronic devices and humans. (Ben Marzouk, 2018)

Cybersecurity, on the other hand, is the practice of defending computers, mobile devices, electronic systems, networks, and data from malicious attacks. It refers to the security of networks, information systems, data, and devices connected to the internet. Thus, it involves the procedures and standards that must be adopted or adhered to in order to face threats and prevent or at least reduce the impact of attacks. (Kandil, 2023)

The U.S. Department of Defense defines cybersecurity as all organizational measures that provide adequate protection for all types and forms of information, whether electronic or physical, from various risks, attacks, crimes, acts of sabotage, espionage, and incidents. The European Commission, meanwhile, defines cybersecurity as "the ability of an information system to resist attempted intrusions or unexpected incidents targeting data." (Al-Shammari, 2020)

Edward Amoroso defined cybersecurity as the tools that reduce the risk of attacks on software, computer devices, or networks, including tools used to combat hacking and detect viruses. (Amoroso, 2007) While he strongly advocated the effectiveness of cybersecurity tools in deterring cybercrimes, he noted that these tools do not always prevent such crimes but can significantly reduce their likelihood and impact.

The Privacy of Digital Data

The concept of digital or informational privacy as a distinct idea can be attributed to American authors Westin Alan and Milar in their work Privacy and Freedom, and in the book The Assault on Privacy. It can be said that the terms "privacy" and "informational (or digital) privacy" are largely synonymous, with the difference being that informational privacy emerged with the advent of the internet, modern communication technologies, and digital environments, while the broader concept of privacy has existed since ancient times—rooted in regulating individual behavior within society and the inherent right to have one’s personal matters respected without interference.

Thus, digital privacy refers to an individual’s right to control the collection of their personal data, its automated processing, storage, distribution, and use in decision-making that affects them. (Abu Hussein, 2021)

Cybercrime

Cybercrime, in its technical sense, refers to information crimes committed using computer technologies either directly or indirectly, with the aim of carrying out a specific criminal act. (Nour Al-Huda, 2023) The U.S. Office of Technology Assessment defines it as "crimes in which computer data and information programs play a central role" (Ihlihhel, 2023), emphasizing the method or tool used in committing the crime. The Association of Chief Police Officers defines cybercrime as involving, or facilitating, the use of computers, the internet, and technology networks in its commission. This definition focuses on the means of committing the crime, specifically identifying the types of tools used in cybercriminal activities. Meanwhile, the Australian Institute of Criminology defines cybercrime as a general term that refers to crimes committed using electronic data or communication devices. (Abdeljawad, 2023) Hence, cybercrime is not limited to targeting data stored on computer systems but includes all criminal activities involving the use of computers, the internet, and various advanced technologies—including artificial intelligence systems employed in fifth-generation (G5) warfare.

Digital Transformation

Digital transformation refers to the cultural, organizational, and operational shift within an institution, industry, or ecosystem through the smart integration of digital technologies, processes, and competencies across all levels and functions in a phased and strategic manner. (i-Scoop) At its core, it involves converting analog information into digital form using an analog-to-digital converter, such as scanners for images or digital audio recordings. Since the rise of the internet in the 1990s, the use of digitization has increased. However, digital transformation extends beyond merely digitizing current processes. (Al Shamsi, 2023) It entails reevaluating and reinventing how products, operations, and institutions work by leveraging emerging digital technologies. It also involves the strategic adoption of digital tools to enhance production processes, improve employee and customer experiences, manage business risks, and control costs. (Aif & Kholoufi, 2022)

Artificial Intelligence (AI)

Artificial intelligence is defined as "a computer system capable of mimicking human behavior, intelligence, performance, and tasks." (Tawfiq, 2023) Others define AI as machines or devices capable of performing tasks that require some form of intelligence, such as understanding cognitive processes like knowledge representation, planning, learning, problem-solving, adaptation, and interaction. Mathematically, this involves implementing these processes within a computer system using the necessary techniques, including algorithms and computational structures. (Tawfiq, 2023)

Simply put, AI is the intelligent imitation of human behavior using robots or machines embedded with thinking systems that replicate human cognition—carrying out tasks like problem-solving, decision-making, speech recognition, translation, and more. (Nasrallah, 2021) These technologies are capable of learning and handling massive volumes of data, transforming them into powerful tools that can anticipate outcomes and make decisions in place of humans—at speeds far beyond human capabilities. (Boubaya, 2021) Evidence of this can be seen in the advancement of AI systems that now include Machine Learning (ML) and Deep Learning (DL), which refer to algorithmic methods by which computers learn how to

perform tasks such as classifying data and predicting values, achieved through the analysis and processing of big data.

The Role of the United Arab Emirates in the Field of Cyber and Digital Security

The United Arab Emirates (UAE) is considered one of the leading countries that has taken significant steps to enhance its cybersecurity practices. Among these initiatives is the adoption of the National Cybersecurity Strategy, which aims to create a secure and resilient cyber environment. This environment is designed to empower individuals to achieve their aspirations and enable businesses to grow and thrive in a safe and prosperous digital space. The UAE supports cybersecurity standards through various mechanisms and strategic pillars and has enacted and implemented advanced laws and regulations to combat cybercrimes, including the new Cybercrime Law of 2021.

In this context, the establishment of the Cybersecurity Council was announced, with the objective of formulating policies and legislation to strengthen cybersecurity in the country and to raise the preparedness of all sectors in responding to cyber threats. In March 2022, the council signed a memorandum of understanding with Deloitte, one of the world's largest professional services firms, to organize frameworks for cooperation between the two parties and build capabilities not only within the UAE but also across the region and globally. This will enable the council to effectively contribute to international efforts to combat and respond to cyber threats.

State Intervention in Enacting Protective Legislation for Achieving Digital Security

The state's intervention across various domains is an expression of its sovereignty. Legislative interventions in the security field aim to ensure protection and enforce its implementation to achieve stability. Therefore, the UAE's legislative involvement in the electronic field seeks to protect against breaches, rumors, and to counter cyber threats—ensuring a sound cybersecurity system. In line with other countries, the UAE has issued a robust legal framework to regulate this domain. (Rajab, 2022)

Content of the UAE Cybercrime Law

Under this 2016 law, anyone who manipulates a network's IP address, uses a fake address, impersonates someone else's IP, or uses any similar methods with the intention of committing a crime or avoiding detection shall be penalized.

This law also ensures legal protection and privacy for the data and information shared or published online. It includes several articles that criminalize violations of privacy via digital means such as eavesdropping, intercepting communications, recording or broadcasting conversations or audio-visual content, taking photos without consent, or producing, transferring, revealing, copying, storing, or publishing any type of digital data or images, even if accurate or truthful. (Al-Humairi, 2023)

Furthermore, the law punishes those who engage in extortion or threats via digital networks to force someone to act or refrain from acting.

To strengthen these measures, the Computer Emergency Response Center was established to improve cybersecurity standards and practices, and to protect the ICT sector's infrastructure from risks and cyberattacks. The center also supports the enhancement of the

Cybercrime Law, the development of new cybersecurity legislation, and the building of national expertise in information security. It manages emergency responses and includes reliable contact centers for reporting cybercrimes and a national center for gathering data on cybercrimes. (Federal Decree Law No. 5 of 2012 on Combating Cybercrimes) (Rajab, 2022)

Undoubtedly, this law has consistently aimed to strengthen digital and electronic security for both citizens and residents within the United Arab Emirates. This is achieved through the Smart Pass service and national ID cards issued by the UAE. Regarding ID cards, all residents of the UAE have been registered by the Federal Authority for Identity and Citizenship as part of the Population Register and Identity Cards project. The registration process relies on individuals' biometric data, which includes unique, non-transferable traits such as palm geometry, fingerprints, retinal scans, and specific facial features.

As for the Smart Pass service (Al-Dabbasa), it provides unified access to all electronic services across government entities in the UAE. This service simplifies the process of completing online transactions by using a single user account and password, eliminating the need for users to create multiple accounts and remember different login credentials for various government portals. It saves users significant time and effort by intelligently identifying them and retrieving their essential information without repeatedly asking for it. Additionally, it reduces the likelihood of forgetting usernames and passwords for different government websites.
Users can log in just once using a single user profile, and to use the Smart Pass, residents and citizens of the UAE must first register by using their UAE-issued ID card.

The Law on Combating Rumors and Cybercrimes
In light of the ongoing threat of terrorism and the prevalence of terrorist crimes in many regions around the world, it is essential to acknowledge that the United Arab Emirates has exerted continuous and determined efforts to combat these dangers. This has been evident throughout various stages of its history and across all international and national levels, with comprehensive procedures and measures applied to confront all forms of terrorism. From this standpoint, it must also be noted that combating terrorism in itself faces many challenges—especially in its traditional forms. So, what about cyberterrorism, which thrives in the digital space due to its wide reach, ease of anonymity, ability to commit crimes without trace, and other characteristics of cybercrime? Therefore, more targeted efforts are required in this domain, without overlooking the role of traditional methods in addressing these threats. In fact, combating cyber threats can often involve applying the same tools and strategies used to counter both electronic and conventional terrorism, while taking into account the unique nature of cyberspace. Within this context, a significant legislative update came with the issuance of a federal decree-law on combating rumors and cybercrimes. (Al-Zaabi, 2021)

The main objective of this law is to provide a comprehensive legal framework aimed at strengthening societal protection against cybercrimes committed via internet technologies and digital platforms. It also seeks to safeguard government websites and databases in the UAE, combat the spread of rumors and fake news, tackle online fraud, and protect privacy and individual rights. (Fadallah, 2020)

The law clearly outlines offenses and penalties for any individual who creates or uses a website or any digital tool to hack, damage, or manipulate government data and information systems, or to publish false information that could harm the interests and security of the UAE. It also addresses other cybercrimes, including the creation or modification of bots to transmit false data within the country, electronic document forgery, tampering with personal data, manipulating medical data, bank accounts, and secret codes; electronic begging; publishing content that violates media content standards; failing to remove illegal content; creating or managing websites for human trafficking, incitement to immorality, dissemination of pornographic content, or offenses against public morals.

The law further criminalizes the transfer, possession, use, or acquisition of illicit funds; cyber fraud; electronic blackmail and threats; defamation and insults; conducting unauthorized surveys or statistical studies; misleading advertisements; promoting unlicensed medical products; organizing or encouraging protests without authorization; incitement against the law; insulting foreign states; and promoting or trafficking firearms, ammunition, or explosives. (Al-Hafidh, 2023)

UAE's Efforts in Enhancing Cybersecurity

The United Arab Emirates places great importance on enhancing cybersecurity and protecting the digital infrastructure of the state, its institutions, and citizens. Several key initiatives have been undertaken in this regard. (Al-Issawi, 2017)

One such effort was the establishment of the Telecommunications Regulatory Authority (TRA), which was created to regulate and oversee the telecommunications and information technology sector, ensuring a safe and secure environment for communications and the internet. Additionally, the UAE launched a National Cybersecurity Strategy aimed at improving the security of the digital infrastructure and protecting the country's critical and sensitive data.

Furthermore, the country has developed and enacted updated laws and regulations related to cybersecurity and the protection of sensitive information, such as the Cybercrimes and Information Technology Law and the Personal Data Protection Law. (Al-Amiri, 2021)

International cooperation has also been a significant part of the UAE's cybersecurity efforts. The country has participated in various global initiatives to exchange knowledge and best practices in cybersecurity, and to collaborate on fighting cybercrimes across different international forums.

In terms of education and capacity-building, the UAE has focused on developing the skills needed to confront cyber threats by offering specialized education and training programs for employees, students, and the general public. (Al-Haidari, 2019)

It is evident that the UAE is actively working through its legislative framework to implement strategies that strengthen its cyber resilience in alignment with global challenges by reinforcing digital infrastructure and preparing for potential cyberattacks.

Methods to Strengthen Cybersecurity in the United Arab Emirates

The information revolution has ushered in significant changes in human civilization, extending across economic, social, political, and cultural spheres. The dissolution of spatial boundaries and the rise of open digital spaces, coupled with the absence of centralized control over cyberspace, have left societies more vulnerable to digital threats. This vulnerability is further exacerbated by security gaps arising from the increasing expertise of users and the rapid development of digital technologies, which deepen the potential risks of cyberattacks. As such, entering digital organizations or workgroups now necessitates digital transformation, the use of strong passwords, and the establishment of robust firewalls to ensure a secure environment.

In this context, the availability of cybersecurity in the United Arab Emirates has become essential to protect the country against hostile actions and the misuse of information and communication technology—especially given the use of cyberspace by terrorist groups for espionage and recruitment. These developments have created new challenges for national security and have underscored the need for coordination and cooperation among security institutions to maintain cybersecurity. (Abdul Ridha & Al-Mamouri, 2020)

Among the technical and electronic methods used to achieve cybersecurity is ensuring the confidentiality, integrity, and availability of information when needed. This involves deploying a variety of technological mechanisms to prevent or mitigate the damage caused by cyber threats. These protective measures vary in nature and purpose and are implemented through procedural means that strengthen investigative and intelligence units within relevant agencies. These tools help identify and apprehend criminals, deter future crimes, and enable the early detection and disruption of terrorist plots through preemptive action based on accurate intelligence.

Thus, technological means play a central role in achieving cybersecurity in the UAE and confronting electronic threats, without underestimating the importance of non-technical measures. The use of such non-technical precautions by security agencies aids computer systems in resisting or neutralizing cyberattacks. (Al-Hamiri, 2023)

Furthermore, the establishment of a center dedicated to information security, incident management, and cybercrime response is of utmost importance. In the face of increasing cyberattacks by extremist organizations that rely heavily on the exchange of information through networks and cyberspace, such a center could reduce terrorist crimes by over 70%. It would also help lower the costs of military operations and reduce human casualties resulting from direct confrontations with cybercriminals. To ensure its operational independence and efficiency, the center should be linked to an independent authority, free from external pressures. This would be achieved by enacting legislation that includes all regulatory, technical, administrative, and financial aspects of its establishment. (Al-Shammari, 2022)

Strengthening Critical Infrastructure Against Cyber Attacks

Although the technical impact of denial-of-service (DoS) attacks may seem relatively minor, their consequences can be devastating at the national level. The potential economic losses a country might suffer from a week-long paralysis due to an internet outage must not be

underestimated. In nations with advanced military systems that rely heavily on network technologies, such attacks can significantly undermine the readiness and effectiveness of those systems. While the effects of these attacks are often confined to cyberspace, the growing use of industrial control systems (ICS) connected to the internet for diagnostics, resets, and administrative functions has created new vulnerabilities. Malicious actors and cybercriminals can now remotely manipulate the operations of gas pipelines, fuel production facilities, chemical plants, and power stations. In any of these scenarios, tampering with the software that governs these systems could result in serious, even global, disruption and damage.

In 2006, the U.S. government's Idaho National Laboratory conducted an experiment demonstrating how a generator at a utility company could be destroyed via an internet-based cyberattack. The generator was connected to a laboratory system designed to replicate the actual infrastructure setup used by electricity providers. The attacker gained remote access to the generator and sent commands that caused it to shudder violently before ultimately exploding. Notably, such generators require six months to manufacture and are produced on a made-to-order basis only. (Al-Hafiz, 2023)

Conclusion

Cyber and digital security represents the protection of the digital world, sensitive information, and data from cyber threats and attacks. It is a vital necessity in our present era, where technology has become an essential part of daily life, business systems, and government operations.

This role is manifested in the protection of systems and networks through the implementation of necessary measures to safeguard computing systems and electronic networks from breaches, unauthorized access, and exploitation of security vulnerabilities. It also involves securing data by protecting sensitive information and personal data from leaks and unauthorized access through proper access policies, encryption technologies, and security tools. Furthermore, it includes responding to cyberattacks by detecting, countering, and mitigating their impact swiftly to restore systems to normal functionality. Cyber awareness is also crucial—educating employees and users on the importance of cybersecurity and guiding them on safe practices to prevent threats.

Study Findings

- Understanding Cybersecurity: The study showed that cybersecurity encompasses a wide range of measures and procedures aimed at protecting electronic systems and sensitive data from cyberattacks. It includes securing devices, networks, and data against various threats.
- UAE's Role in Enhancing Cybersecurity: The study concluded that the United Arab Emirates has taken significant steps to bolster cybersecurity, including the development of a national cybersecurity strategy, the establishment of the Telecommunications Regulatory Authority (TRA), and the enactment of laws such as the Cybercrimes Law and the Personal Data Protection Law.
- Strategic Analysis: The study revealed that the UAE has established clear strategies to enhance cybersecurity. These include improving digital infrastructure, developing

necessary legislation, fostering international cooperation, and advancing education and training in cybersecurity.

- Assessment of Cyber Defense Readiness: The study indicated that the UAE has strong cyber defense readiness, capable of countering cyber threats, supported by coordinated governmental efforts and collaboration with international companies to strengthen cybersecurity capabilities.
- Challenges and Opportunities: The study identified key challenges facing the UAE in the cybersecurity domain, including increasing and complex threats and the rapid pace of technological advancement. Conversely, digital transformation and technological innovation offer opportunities to enhance cybersecurity and boost electronic protection.
- Laws and Initiatives: The study highlighted that the UAE has enacted a robust legal framework to combat cybercrimes and protect sensitive data, with a focus on developing workforce skills through continuous education and training.
- Importance of Cyber Awareness: The study emphasized the critical role of cyber awareness among employees and users as a core component of cybersecurity strategies to promote safe practices and prevent cyber threats.

Overall, the study enhances comprehensive understanding of cybersecurity and sheds light on the substantial efforts made by the United Arab Emirates to protect its digital infrastructure and strengthen its cybersecurity posture in the face of escalating threats.

References

Abdeljawad, N. A. A. (2023). Cybercrime and its impact on Egyptian national security: A socio-analytical study. Faculty of Arts Journal, 15(1).

Abdel Sadeq, A. (2019). Cyber terrorism: Power in international relations – A new pattern and different challenges. Center for Political and Strategic Studies.

Abu Hussein, H. J. (2021). Legal framework for cybersecurity services: A comparative study (Unpublished master's thesis). Middle East University, Amman.

Afif, H., & Kholoufi, W. (2022). The trend toward digital transformation: Necessity or choice. Journal of Money and Business Economics, 6(1), 276–291.

Al-Amri, M. S. (2021). Cybersecurity and digital investigations. Union Press and Publishing.

Al-Dabbasa. (n.d.). [Details missing; provide publication info if available].

Al-Haidari, Z. (2019). Cybersecurity – Risks, challenges, and confrontation. Dar Al Sharq for Printing and Publishing.

Al-Hafidh, M. B. (2023). Law on combating rumors and cybercrimes in the UAE. Dar Al-Hafidh Series for the UAE.

Al-Humairee, S. A. N. (2023). The role of cyber safety and digital security in the United Arab Emirates. Al-Baheth Journal of Legal and Judicial Studies, (58), 517–538.

Al-Issawi, H. M. (2017). [Title missing; please verify source information].

Al-Muhairi, A. A. (2023). The role of the UAE in achieving cybersecurity. Journal of Scientific Readings in Legal and Administrative Research, (20), 441–471.

Al-Shammari, S. M. H. (2020). Cybersecurity as a new pillar in Iraqi strategy. Political Issues, 12(62), 273–296.

Al-Shammari, S. M. H. (2022). [Title missing; please verify source information].

Al Shamsi, M. (2023). Digital transformation in education: The United Arab Emirates as a model. Journal of Islamic Entrepreneurship, 8(1), 11–21.

Al-Zaabi, S. A. S. (2021). Mechanisms for combating cybercrime in the UAE. Moroccan Law Journal, (46).

Amoroso, E. (2007). [Title missing; please verify source information].

Bara, S. (n.d.). Cybersecurity in Algeria: Policies and institutions. Algerian Journal of Human Security, (2).

Boubayaa, N., & El Wafi, S. (2021). Big data analysis using artificial intelligence techniques in auditing. Journal of Economic Integration, 9(9) (3).

Ehlihil, K. (2023). Cybercrime and international efforts to confront it. International Electronic Journal for Legal Research, 1(3).

Fadlallah, F. M. A.-H. (2020). Crime of violating privacy in UAE legislation: An analytical study. Journal of In-Depth Legal Research, (44).

Federal Decree-Law No. 5 of 2012 on Combating Cybercrimes.

Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrimes (Issued on January 2, 2022).

Kandil, A. A. (2023). Mechanisms for achieving information security in the UAE. Police Thought Journal, 32(126), 185–229.

Nasrallah, N. M. (2021). Using artificial intelligence (AI) in banking services. Introductory Booklet Series, (24).

Nour El Huda, Q. (2023). Cybercrime and mechanisms to combat it: Facing cybersecurity challenges. Algerian Journal of Law and Political Science, 8.

Rajab, Y. M. A. (2022). Emerging legislative developments in information security: A comparative study. Arab Journal of Informatics and Information Security, (6), 115–152.

Tawfik, S. E. M. (2023). Artificial intelligence: An approach to enhancing academic excellence in Egyptian universities: A foresight study. Journal of Educational Sciences, 31(1).