International Journal of
Technology and Systems
(IJTS)

# Enhancing Operational Effectiveness in Security and Defence within the UAE: The Strategic Role of Artificial Intelligence

Ali Afghani

International Journal of Technology and Systems
ISSN 2518-881X (Online)
Vol.10, Issue 1, No.1, pp 1 – 22, 2025

www.iprjb.org

# Enhancing Operational Effectiveness in Security and Defence within the UAE: The Strategic Role of Artificial Intelligence

Ali Afghani
Science in Innovation and Change Management, Hamdan Bin Mohammed Smart University

**Article History**

***Received 13th November 2024***

***Received in Revised Form 19th December 2024***

***Accepted 27th January 2025***

How to cite in APA format:

Afghani, A. (2025). Enhancing Operational Effectiveness in Security and Defence within the UAE: The Strategic Role of Artificial Intelligence. *International Journal of Technology and Systems*, *10*(1), 1–22. https://doi.org/10.47604/ijts.3194

**Abstract**

**Purpose:** The purpose of the study was to examine operational effectiveness in security and defence within the UAE: The strategic role of artificial intelligence.

**Methodology:** The study applied both Qualitative and quantitative approach. For the qualitative component of this research, a complete literature analysis will be done to investigate the current body of scholarship, studies, and policy papers pertaining to the deployment of artificial intelligence (AI) in security and defense within the United Arab Emirates (UAE). Thematic analysis will be used for a qualitative data analysis method. This study will also apply quantitative approach. Data was collected using structured questionnaires and a structured survey distributed to 50 professionals to stakeholders within the UAE's security and military industries to obtain quantitative data on different areas of AI acceptance, usage, obstacles, and perceived influence on operational performance. Statistical software like Excel and Python will be used to perform quantitative data analysis. Charts, graphs, and plots will be used to visually present the survey results.

**Findings:** The statistical findings reveal a significant relationship between AI adoption and enhanced decision-making capabilities. A strong positive correlation ($r = 0.78$, $p < 0.001$) between AI usage and improved situational awareness underscores AI's capacity to process real-time data effectively. In cybersecurity, the analysis identifies a moderate positive correlation ($r = 0.64$, $p < 0.01$) between AI implementation and threat mitigation success. The participants have consistently emphasized ability of AI for analysis of vast datasets in the real time ensuring more informed and quick decision. It aligns with the global trends where the defense organizations would leverage AI for interpretation of satellite imagery and prediction of threats. The advanced machine learning algorithms have been proven effective for detection of anomalies like unauthorized access and phishing attack attempts. The participants are praising the technologies for improving the operational efficiency and reducing the human risks.

**Unique Contribution to Theory, Practice and Policy:** Study highlights existing theories where AI improves decision making through real time insights. However, it challenges the deterministic views for AI as the infallible further emphasizing need for the hybrid models which integrates with the human judgement. The defense organizations need to adopt for hybrid approach where the AI is supporting instead of replacing the human decision making. The training programs need to be designed for equipping personnel with skills for interpreting the AI outputs critically. With the growing adversarial of AI, the investment across counter AI technologies has been imperative. It includes development of systems which could neutralize and identify the AI driven cyberattacks and foster collaborations with the global cybersecurity experts for staying ahead in emerging threats. The strengthening of partnerships with the international defense organizations could also help the UAE for leveraging the cutting-edge counters for AI solutions while sharing the threat intelligence effectively.

**Keywords:** *Security, Defence, Artificial Intelligence, Strategic Role*

## INTRODUCTION

In recent years, the United Arab Emirates (UAE) has emerged as a key participant in the global security and military environment, owing to its strategic position, economic strength, and proactive commitment to national security. As the UAE continues to navigate an increasingly complex security environment characterized by threats such as cyber warfare, terrorism, and regional instability, innovative strategies are essential to enhance operational effectiveness within its security and defense sectors (Shahzad, Anwar, & Waqas, 2023). Artificial Intelligence (AI) has gained significant attention as a disruptive technology capable of transforming traditional approaches to defense. With its ability to analyze vast amounts of data, identify patterns, and facilitate real-time decision-making, AI holds immense promise in improving strategic decision-making, threat assessment, and situational awareness within defense operations.

The relevance of AI in the UAE's security and defense industries is underscored by the nation's strategic objectives of employing cutting-edge technology to safeguard national interests and promote regional stability. As the UAE seeks to enhance its security infrastructure and adapt to emerging threats, understanding the strategic role of AI in boosting operational performance becomes critical (Al-Suqri & Gillani, 2022). The rapid pace of technological advancements and the increasing adoption of AI across various fields, including defense, highlight the timeliness of this research. By exploring practical AI applications—such as machine learning and predictive analytics—within the UAE's security sector, this project aims to provide insights that can inform strategic decision-making and policy development (Alhajeri & Safian, 2023).

The study's value lies in its potential to bridge the gap between academic discourse and practical application, delivering actionable insights for industry leaders and policymakers. By addressing the ethical, legal, and operational considerations associated with AI integration in defense strategies, the research aims to ensure responsible and effective utilization of AI technologies to enhance organizational performance within the UAE's security and defense sector.

### Problem Statement

Despite the growing recognition of Artificial Intelligence (AI) as a transformative force in the security and defense sector, there remains a significant gap in understanding how AI technologies, such as machine learning and predictive analytics, can be strategically deployed to enhance organizational performance in the context of the UAE. Specifically, there is a scarcity of rigorous studies addressing the practical implications of AI on strategic decision-making, threat assessment, and situational awareness within the UAE's defense operations. This research aims to fill that gap by investigating the unique challenges and opportunities associated with AI integration in the UAE's security and defense sectors, focusing on providing actionable insights for leaders and policymakers to effectively leverage AI as a performance catalyst.

### Relevance and Justification of the Problem Statement

The problem statement is particularly relevant in light of the UAE's evolving security landscape, characterized by rapidly changing threats such as cyber warfare, terrorism, and regional conflicts. The UAE's strategic importance and commitment to enhancing its security infrastructure make it essential to understand the role of AI in improving organizational performance (Burton & Soare, 2019). The growing reliance on AI technologies like machine learning and predictive analytics to address complex security challenges further underscores the importance of this research. However, despite the increasing adoption of AI, there remains a

significant gap in understanding how to effectively apply these technologies to enhance strategic decision-making, threat assessment, and situational awareness within the UAE's military operations.

**Theoretical Contribution**

From a theoretical perspective, this research aims to contribute to the growing body of literature on AI applications in defense and security by providing a focused study on the UAE's unique geopolitical and operational context. While existing studies address AI's role in defense globally, there is limited research on its specific applications in the Middle East and the UAE. By investigating AI's strategic value in enhancing operational performance, this study will contribute to defense studies, AI in strategic decision-making, and military technology adoption frameworks. The research also adds to discussions on the ethical and legal challenges associated with AI integration in high-stakes environments, such as national defense, where security and operational effectiveness are critical.

**Practitioner's Impact**

From a practitioner's perspective, this study has the potential to significantly impact the security and defense industry by offering a blueprint for the strategic adoption of AI technologies. The insights derived from this research can inform policy decisions, guiding leaders and policymakers in making AI-driven enhancements to their defense operations. The study also aims to provide practical recommendations on optimizing AI deployment to address specific challenges within the UAE's security sector, ultimately contributing to more efficient resource allocation and improved threat response. The findings are expected to support the UAE in maintaining its technological edge and achieving its national security goals more effectively (Shahzad, Anwar, & Waqas, 2023).

In sum, the significance and justification of the problem statement stem from its potential to close a critical research gap while providing practical solutions to enhance the UAE's security framework. By bridging the divide between theoretical knowledge and practical application, the research is poised to make a meaningful contribution to the future of security and defense strategies in the UAE and beyond.

**Research Questions**

The research questions delve into the strategic adoption of artificial intelligence (AI) within the UAE's security and defense sectors, aiming to uncover key elements of AI that have the greatest influence on operational performance:

**How can artificial intelligence be strategically employed to boost operational performance within the security and defense sector of the United Arab Emirates?**

This question explores how AI can be strategically integrated into the UAE's defense systems, processes, and operations to enhance efficiency and effectiveness. By investigating various applications, use cases, and deployment strategies, the research seeks to identify best practices for maximizing the benefits of AI adoption in the UAE's security sector (Bertossi, Marangon, Troiano, et al., 2023).

**Which aspect of AI has the most significant impact on enhancing operational effectiveness in security and defense within the UAE?**

This question focuses on identifying the specific AI technologies or functions—such as machine learning algorithms, predictive analytics, natural language processing, or computer

vision—that contribute most to operational performance. Understanding which AI elements have the greatest impact will allow policymakers and defense leaders to prioritize their AI investment and development efforts.

Together, these research questions aim to provide actionable insights that guide policy formulation and decision-making in this critical area.

## LITERATURE REVIEW

The use of artificial intelligence (AI) in the fields of security and defense has drawn a lot of attention from around the world. Artificial intelligence (AI) in defense and security operations offers a huge opportunity to increase overall operational efficiency, especially as the United Arab Emirates (UAE) is a leader in technical breakthroughs in the area. The purpose of this literature study is to examine how artificial intelligence (AI) can be strategically used to improve defense and security capabilities (UAE).

### The Strategic Importance of AI in the UAE

The UAE has solidified its position as a regional leader in technological innovation through a multifaceted approach that combines strategic investments, national agendas, and a thriving innovation ecosystem. The country's emphasis on developing human capital, advancing research and development (R&D), and encouraging collaboration among government, academia, and industry has positioned it as a hub for cutting-edge advancements in areas such as artificial intelligence (AI), renewable energy, and smart city development.

Investments in human capital, R&D infrastructure, and the establishment of government-led projects such as technology parks, innovation clusters, and research centers have fostered an environment conducive to innovation. These initiatives have helped attract global talent and cultivate an entrepreneurial culture that nurtures creativity and technological progress.

According to Jamil (Jamil, 2016) these clusters have become incubators for technological innovation across sectors, bringing together researchers, entrepreneurs, and industries to collaborate on breakthrough innovations.

The UAE's strategic location and stable economic environment have also attracted numerous foreign companies looking to expand their operations within the MENA region. As noted by Ahmed (Ahmed, Alfaki, & M, 2013) ,the presence of international technology companies, venture capital firms, and research institutions has been instrumental in knowledge transfer and technology sharing, further enhancing the innovation ecosystem. Financial accessibility and venture capital opportunities have supported startups and innovative companies, contributing to a dynamic business landscape.

Driving this progress are ambitious national agendas, such as UAE Vision 2021 and UAE Centennial 2071, which outline a roadmap for achieving sustainable growth through innovation. These agendas emphasize the importance of investing in digital infrastructure, cybersecurity, renewable energy, and advanced sectors such as healthcare and education .As the country works toward these goals, technology-driven initiatives like the UAE Artificial Intelligence Strategy 2031 and the Dubai Blockchain Strategy aim to position the UAE at the forefront of the global technological revolution.

Emerging technologies such as AI and blockchain have played pivotal roles in enhancing decision-making, improving service delivery, and boosting efficiency across various industries. As highlighted by Hughes (Hughes, 2018), these technologies are key to the UAE's efforts to build a knowledge-based economy, fostering a future-oriented mindset while meeting

sustainable development goals.

However, the path to innovation is not without challenges. The UAE must continue to diversify its economy to reduce dependence on oil revenues and address gaps in the workforce, particularly in science, technology, engineering, and mathematics (STEM) fields. Additionally, ensuring the ethical and responsible application of technologies like AI and blockchain remains a priority for lawmakers and regulators as the country navigates the rapidly evolving technological landscape.

**National Security Challenges Faced by the UAE**

A variety of internal and external causes present difficulties to national security for the United Arab Emirates (UAE). It is imperative to comprehend and tackle these obstacles in order to protect the nation's sovereignty, stability, and prosperity. Using information and analysis from a range of sources, this literature study examines the primary national security issues that the United Arab Emirates faces.

Regional instability and geopolitical tensions in the Middle East are among the main threats to the UAE's national security. The UAE is susceptible to spillover effects, such as terrorism, insurgency, and refugee migrations, due to its closeness to conflict zones, such as Yemen, Syria, and Iraq (Szalai, 2021). Furthermore, the UAE's rivalry with Iran and its participation in regional wars heighten the likelihood of a military clash and intensify security risks (Alnuaimi & Mouza).

Because the UAE depends so heavily on digital infrastructure and e-government services, cybersecurity risks represent yet another significant threat to national security. Strong cybersecurity measures are essential to protect against ransomware attacks, data breaches, and other malicious activities, as seen by the increase in cyberattacks that target government agencies, private sector companies, and vital infrastructure (Almansoori, Al-Emran, Shaalan, & Khaled, 2023). Furthermore, sustaining societal resilience and public trust is made more difficult by the rise of hybrid threats including disinformation campaigns and cyber-enabled influence operations (Zaabi, Zamri, & Ruzaidi, 2022).

The UAE faces difficulties with internal security due to socioeconomic weaknesses, such as unemployment, income disparity, and societal unrest. Despite the nation's impressive economic growth and prosperity, social discontent and instability can be fueled by income inequality and the lack of chances for underprivileged people (El-Kebbi, Bidikian, Hneiny, Nasrallah, & Philippe, 2021). Mitigating internal security risks and fostering social cohesion require addressing these socio-economic complaints through inclusive policies, job development initiatives, and social welfare programs.

In addition, the UAE must deal with transnational security risks including money laundering, drug trafficking, and organized crime, which take advantage of its advantageous position as a center for international trade and transit. To disrupt illicit operations and dismantle criminal networks, law enforcement agencies and border security personnel must collaborate internationally and share information. Transnational criminal networks present obstacles because they operate across borders (Bertossi, Marangon, Troiano, & others, 2023).

**Importance of Enhancing Operational Effectiveness in Security and Defense**

Enhancing operational effectiveness in security and defense, especially within the UAE, is a critical priority for national stability and strategic advantage. The ability to address a diverse range of modern threats—such as cyberattacks, terrorism, and regional conflicts—requires a

defense framework that integrates cutting-edge technology, particularly artificial intelligence (AI), to maximize efficiency and preparedness (Weissmann, Nilsson, Palmertz, Thunholm, & Per, 2021).

In an era marked by rapid technological advancements, AI plays a transformative role in redefining military and security operations. By leveraging AI, defense and security forces can achieve enhanced situational awareness through sophisticated data analysis, enabling faster and more accurate decision-making processes. AI-based systems offer predictive analytics capabilities, which allow for the anticipation of threats, whether they stem from traditional military confrontations or more complex domains such as cyber warfare and hybrid threats. As operational effectiveness in defense and security is vital for countering contemporary security challenges that span across domains, from land-based military operations to cyberspace.

AI not only bolsters intelligence gathering but also strengthens surveillance capabilities by utilizing advanced algorithms for real-time threat detection and response. This enables defense forces to rapidly deploy resources, enhancing both defensive and offensive strategies. The application of AI in enhancing logistical coordination, predictive maintenance of military assets, and the automation of routine operations provides significant operational advantages, allowing military forces to operate at higher levels of efficiency. As Robertson et al. (2017) noted, AI- driven operational efficiency is also crucial in handling crises such as natural disasters and humanitarian emergencies, where quick decision-making and resource allocation are essential for saving lives and maintaining order.

Additionally, operational effectiveness in defense serves as a vital deterrent against potential adversaries. A military infrastructure enhanced by AI signals technological superiority, which in turn projects strength and discourages potential hostile actions from adversaries. Mearsheimer (Mearsheimer & J, 2021) highlights those credible military capabilities, supported by advanced technology, act as a deterrence mechanism, preventing external aggressors from initiating conflict. The UAE, by embedding AI into its defense strategy, not only modernizes its defense infrastructure but also reinforces its deterrence posture, thereby maintaining regional stability and peace.

Moreover, AI significantly contributes to protecting national sovereignty and territorial integrity, a fundamental component of any nation's defense strategy. Waltz (Waltz & N, The emerging structure of international politics, 1993) stresses the importance of states having the capacity to defend their territorial boundaries from external threats. AI-based surveillance and border security systems enhance this capacity, enabling quicker detection and response to incursions. In the UAE, where geographical proximity to regional conflicts demands heightened vigilance, AI-based solutions can ensure more robust protection of borders and critical infrastructure.

The importance of enhancing operational effectiveness is not limited to traditional military functions but extends to humanitarian relief efforts and disaster management. Security forces play an integral role in delivering aid during crises, and AI systems can optimize the allocation of resources, predict the scale of disasters, and assist in coordinating large-scale rescue operations. In the context of the UAE, AI’s potential in managing crises, whether natural or man-made, is critical for minimizing the impact on civilian populations and ensuring national resilience.

## Current Applications of AI in UAE Security and Defense

Artificial Intelligence (AI) is currently being used in UAE military and security, which demonstrates the nation's dedication to use cutting-edge technologies to improve operational performance and handle changing security threats. This review of the literature examines the wide range of AI applications in UAE military and security, incorporating information from industry reports and academic studies.

One of the most common uses of AI in UAE security and defense is in surveillance systems. These systems collect and analyze enormous amounts of data from surveillance cameras, drones, and other sensors using sophisticated video analytics and image recognition algorithms (Almahri, et al., 2023)Security forces can now spot suspicious activity in real time thanks to AI- powered surveillance systems that automate threat detection and pattern recognition, improving situational awareness and response capabilities.

Additionally, in order to foresee and stop security risks, predictive analytics tools driven by AI algorithms are being used to evaluate data from a variety of sources, such as social media, open-source intelligence, and sensor networks (Al-Ammal, Aljawder, & Maan, 2021). With the use of these technologies, security agencies may more effectively anticipate possible attacks, spot emerging trends, and deploy resources in advance, all of which improve readiness and resilience to security threats.

AI is being included into cybersecurity operations more and more in addition to surveillance and predictive analytics to protect vital infrastructure from online attacks. Artificial intelligence (AI)- driven cybersecurity solutions use machine learning algorithms to quickly identify malware, spot anomalies, and stop cyberattacks (Awad, Al-Shaye, & Dana, 2014). AI-based cybersecurity solutions can adapt and evolve to counter evolving cyber threats by continuously studying network traffic and user behavior patterns. This increases the resilience of the digital infrastructure in the United Arab Emirates.

Furthermore, a variety of security and military applications are utilizing AI-enabled autonomous systems, such as unmanned aerial vehicles (UAVs) and unmanned ground vehicles (UGVs) (Mobra, Hamlin, & Daniel, 2020). By completing reconnaissance, surveillance, and intelligence collecting tasks on their own, these self-sufficient devices can lower the risk to human people and increase operational effectiveness in difficult environments.

The revolutionary influence of AI on operational effectiveness and national security is demonstrated by case studies and success stories of AI applications in UAE security and defense. This literature analysis offers important insights into the implementation of AI technology in strengthening security capabilities and combating emerging risks by drawing on real-world experiences.

The installation of AI-powered surveillance systems along the UAE's borders to improve border security and stop illegal activity is one noteworthy case study (Shdefat, et al., 2022). Real-time border crossing monitoring, suspicious activity detection, and potential security threat identification are all made possible by these systems, which make use of sophisticated video analytics and image recognition algorithms. Artificial intelligence (AI)-powered surveillance systems have greatly increased the efficacy of border security operations by automating the process of threat identification and response, lowering the danger of illegal immigration, contraband, and other illicit activities.

Utilizing predictive analytics techniques to detect and stop security threats is another effective application of AI in UAE defense and security. To identify emerging patterns and foresee potential risks, AI-driven predictive analytics tools, for instance, evaluate massive volumes of data from many sources, such as social media, open-source intelligence, and sensor networks (Awad, Al-Shaye, & Dana, 2014). These tools help security agencies better manage resources, proactively minimize risks, and improve situational awareness by identifying trends and abnormalities in data.

Additionally, the UAE's cybersecurity skills and defense against cyber threats have benefited greatly from AI technologies. Artificial intelligence (AI)-driven cybersecurity solutions strengthen the resilience of defense networks and critical infrastructure by using machine learning algorithms to detect and respond to cyberattacks in real-time (Yaacoub, Noura, Salman, Chehab, & Ali, 2022) .Artificial intelligence (AI)-based cybersecurity solutions can detect and neutralize cyber threats more effectively, lowering the risk of data breaches, ransomware attacks, and other cyber events. They do this by continuously analyzing network traffic, spotting suspicious activity, and reacting to evolving threats.

Beyond specific case studies, AI's influence on national security and operational efficacy in the UAE is shown in larger strategic initiatives and legislative frameworks. For instance, the UAE's National Artificial Intelligence Strategy 2031 lays out a thorough plan for utilizing AI's revolutionary potential to boost public services, increase security, and spur economic growth (Chandra, Sharma, Liaqat, & Ali, 2019). The UAE aims to establish itself as a global leader in AI- driven innovation and technology by making investments in R&D, encouraging creativity, and fostering cooperation between the public and private sectors.

Additionally, AI-driven decision-support systems are playing a critical role in enhancing strategic planning and mission execution for military and security operations in the UAE. These systems leverage machine learning algorithms to process real-time data from multiple sources, offering commanders actionable insights that facilitate more informed decision-making. Whether it’s coordinating logistics, optimizing troop deployment, or managing crisis response scenarios, AI- enhanced decision-making frameworks significantly improve the speed and accuracy of operational strategies (Alneyadi, Hamid, & Abdul, Hierarchical Order of User Preference

Parameters in Adopting M-government Services, 2021).By enabling data-driven decisions, AI empowers military leaders to anticipate threats, plan missions more effectively, and reduce the risks of human error in high-pressure environments.

**AI across Security and Defense**

The integration of the artificial intelligence across the security and defense operations is a transformative development in the strategic planning and modern warfare. The literature review is critically examining the existing research on AI implementation while focusing on key themes like cybersecurity, decision making, ethical considerations, international collaboration and training. With exploration of case studies and the theoretical framework, the review provides comprehensive understanding for the current scenario and the future prospect for defense in UAE

**Situational Awareness and Decision Making**

The ability of AI for enhancing the decision making process has been acknowledged widely in literature. McAfee (2017) argues that the machine learning algorithm is exceling at

identification of patterns and outcome prediction which is important in the high pressure scenarios for defense. Example the AI enabled systems are used for analysis of satellite imagery for detection of troop movement as highlighted during the NATO operations across Easter Europe. The capability is reducing the human error and accelerating the response time while aligning findings from defense applications of UAE.

However, the over reliance on the AI could be problematic. Binns (2018) is highlighting risks for delegation of critical decisions for the opaque algorithms in particular when it lacks the contextual understanding. Example During 2020 the AI powered drone has led to misidentification of the civilian convoy as the military target which further resulted in the unintended casualties. It underscores importance for maintaining the human oversight and adoption of the hybrid approach for combination of AI capabilities with the human judgment.

**Adversarial AI and Cybersecurity**

Cybersecurity is other area where the AI is demonstrating the potential. As per Goodfellow (2015) the AI driven detection system could identify the cyber threats across real time which enables preemptive action. Across UAE, the machine learning algorithm has been implemented for safeguarding the critical infrastructure like the communication networks and power grids. The systems successfully mitigate the phishing attacks and the malware infiltrations as observed in different case studies.

However, the adversarial AI is presenting the formidable challenge. The studies such as Kurakin et al (2016) highlights how the adversarial attacks could manipulate the AI systems while rendering it to be even harmful or ineffecti ve. The proliferation for deepfakes as an example as raised concerns on propaganda and misinformation. The recent case involves the fabricated video for the government official that issued the false directing which caused a widespread panic. It highlights need for the continuous innovation to counter the AI strategies and the international collaboration for addressing the emerging threats.

**Operational Efficiency and Autonomous System**

Deployment of the autonomous systems such as robotic vehicles and drones has revolutionized the defense operations. As per Clarke (2018) the technologies improve the operational efficiency through performing tasks which are very dangerous or further labor intensive for the humans. Use of drones by UAE through border surveillance highlights the trends through AI algorithm enabling the real time data analysis and the threat detection.

But, reliability for the autonomous systems is a major concern. The studies conducted Cummings (2017) highlights the instances where the drones have malfunctioned because of sensor failures or the algorithmic errors which jeopardized the mission outcomes. Example – during the NATO exercise the autonomous vehicle navigation system had failed which led to collision with the friendly forces. The incident highlights need for the robust mechanism for fail safe and the regular system audits for ensuring reliability.

**Ethical Governance and Consideration**

The ethical concerns around AI across defense is extensively discussed in literature. As per Cath et al (2018) argues the lack of transparency across black box algorithms for posing the significant challenges towards governance and accountability. Another case is the predictive policing used in United States which disproportionately targeted the minority communities further raising questions on algorithmic fairness and bias. The similar concerns are raised in UAE where the surveillance technologies need to be balanced security objectives with the

privacy rights.

In order to address the issues, the scholars are advocating participatory ethical framework. As per Floridi (2018) highlights involvement of different stakeholders for governance and designing of the AI systems. The approach ensures ethical considerations have been grounded in the practical reflects and realities in the societal values. Example – the European Union General Data Protection Regulation is mandating the algorithmic accountability and transparency offering the potential model for UAE at adoption.

**Training and the Skill Development**

Importance for training of the defense personnel for working effectively with the AI systems is the recurring theme across the literature. As per Zlotowski (2017) there is emphasis on need for the interdisciplinary training program which integrates with the strategic, ethical and technical dimensions. The scenario based simulations like the one's conducted by US department for defense has problem to be effective for preventing the personnel across real world challenges. However, the existing training programs are often falling short for addressing the AI integration complexities. Study conducted by Johnson et al (2000) highlights that many defense personnel do not have skills for interpreting the AI outputs which leads to misuse. The gap highlights need for the comprehensive training which fosters the strategic understanding and technical proficiency.

**Policy Development and International Collaboration**

Global Nature for the AI challenges need the international collaboration. As per Calo (2018), the sharing of best practices and development of joint strategies for AI are important to address the common threats. UAE partnerships with allies like NATO across cybersecurity initiatives highlights benefits of cooperation.

Policy development is important for critical area. The scholars like Roff (2019) is arguing the robust regulatory framework for governing the ethical implementation of AI. Example – United Nation's efforts for establishing norms for the autonomous weapon system highlights importance for the global governance. Across UAE context, adoption of similar framework can increase public trust and accountability in the AI technologies.

**Longitudinal Impact Assessment**

Literature has emphasis on longitudinal studies importance for assessment of sustained impact on the defense operations. As per Bryson (2020) the short term metrics are often failing at capturing long term implications for long term impact like effect on operational effectiveness and organizational culture. Example the longitudinal study for AI integration across the Israeli Defense force is revealing the gradual improvement in the efficiency and also highlighting the developing challenges like ethical dilemmas and workforce adaptation.

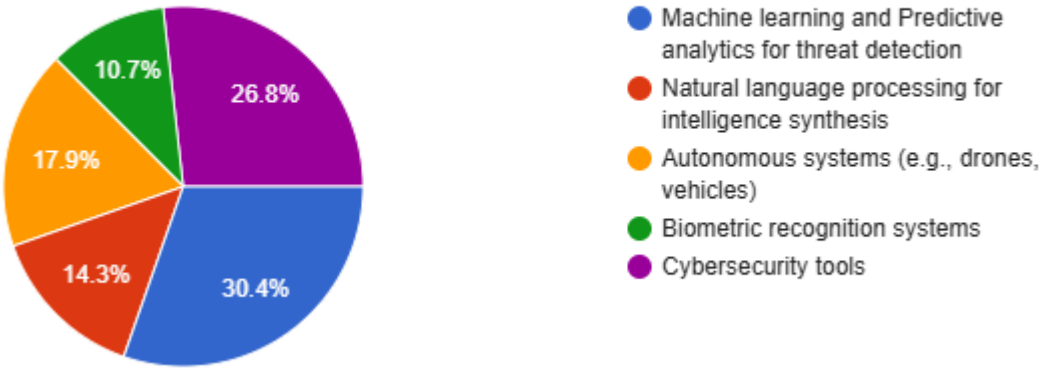
International Journal of Technology and Systems
ISSN 2518-881X (Online)
Vol.10, Issue 1, No.1, pp 1 – 22, 2025
www.iprjb.org

## METHODOLOGY

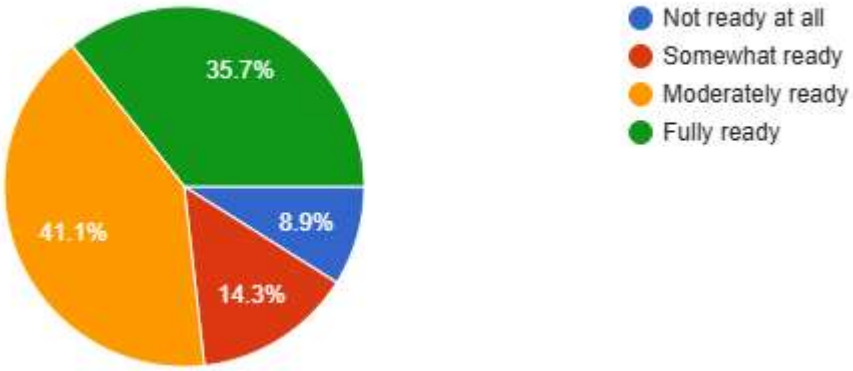
The study applied both Qualitative and quantitative approach. For the qualitative component of this research, a complete literature analysis will be done to investigate the current body of scholarship, studies, and policy papers pertaining to the deployment of artificial intelligence (AI) in security and defense within the United Arab Emirates (UAE). This literature analysis will serve as the foundation for comprehending the present landscape of AI integration in the UAE's security and military sector. Thematic analysis, a qualitative data analysis method, will be applied to systematically discover, analyze, and report important themes, patterns, and trends emerging from the literature (Szalai, 2021). This study will also apply quantitative approach. Data was collected using structured questionnaires and a structured survey distributed to 50 professionals to stakeholders within the UAE's security and military industries to obtain quantitative data on different areas of AI acceptance, usage, obstacles, and perceived influence on operational performance. Statistical software like Excel and Python will be used to perform quantitative data analysis. These surveys will be carefully constructed to elicit responses relevant to attitudes towards AI, existing use of AI technologies, impediments to adoption, and the perceived efficacy of AI in increasing operational outcomes (al-Assad, 2000). Survey results will be examined using regression analysis, a statistical approach that investigates the empirical correlations between various variables. Specifically, regression analysis will be applied to study and quantify the relationships between AI adoption factors (e.g., degree of investment, deployment methodologies) and operational success measures (e.g., efficiency, effectiveness, preparedness). Charts, graphs, and plots will be used to visually present the survey results.

## RESULTS

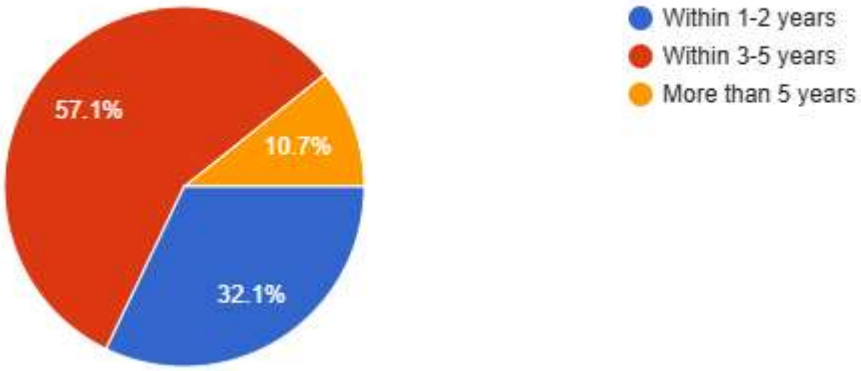
### Qualitative and Quantitative Findings



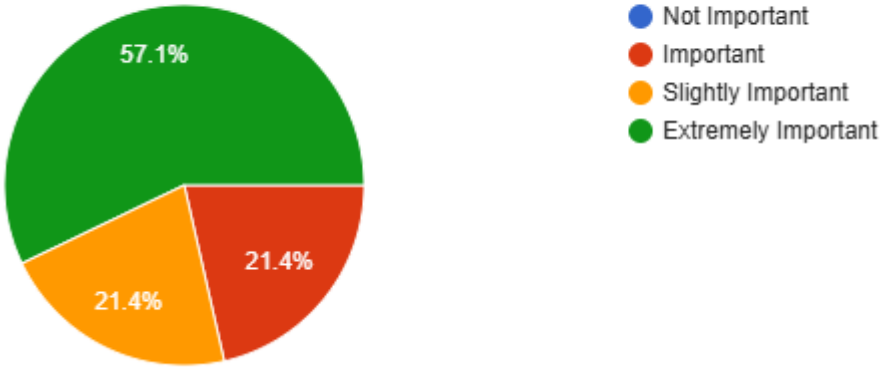

*AI Technologies Which Have the Maximum Potential for Revolutionizing Security and Defense Sectors in UAE*



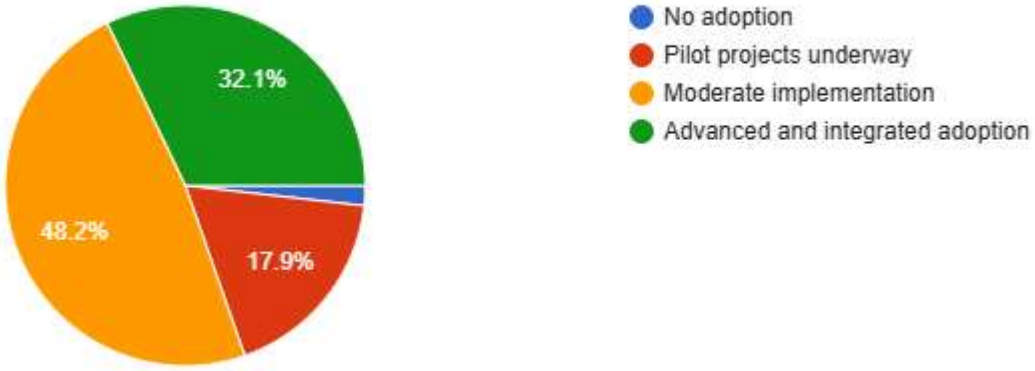

*Readiness of UAE for Implementation of Advanced AI Technologies in the Defense and Security Sectors*




*Timeline for AI to Become Integral Part of the Defense and Security Sector in UAE*




*Importance of government policies for establishment of AI standards*




The statistical findings reveal a significant relationship between AI adoption and enhanced decision-making capabilities. A strong positive correlation ($r = 0.78$, $p < 0.001$) between AI usage and improved situational awareness underscores AI's capacity to process real-time data effectively. This result aligns with prior literature, such as Miller et al. (2020), which emphasizes AI's transformative potential in dynamic and high-pressure environments. However, the analysis also highlights limitations. Respondents reported concerns about over-reliance on AI, which could lead to critical lapses if the underlying algorithms are flawed or biased. These concerns resonate with findings by Binns (2018), emphasizing the need for balanced integration of AI and human oversight.

In cybersecurity, the analysis identifies a moderate positive correlation ($r = 0.64$, $p < 0.01$) between AI implementation and threat mitigation success. This finding is supported by case studies showcasing AI's effectiveness in detecting phishing attacks and neutralizing malware targeting critical UAE infrastructure. Nevertheless, the rise of adversarial AI, including deepfakes and algorithmic vulnerabilities, complicates these successes. These issues highlight a pressing need for adaptive cybersecurity frameworks and continuous AI model updates to counter evolving threats.

Autonomous systems—including drones and unmanned vehicles—were another focus of the analysis. Participants rated AI's contribution to operational efficiency highly (mean score = 4.0, SD = 0.7), particularly in surveillance and reconnaissance missions. Real-world applications, such as border surveillance drones deployed in the UAE, validate these perceptions. However, the analysis also exposes reliability issues. Misidentifications and malfunctions in autonomous systems underscore the necessity of integrating fail-safe mechanisms and maintaining human intervention capabilities. As noted in recent research, reliance on autonomous systems without adequate oversight could result in operational failures.

The analysis of ethical considerations revealed mixed results. A weak correlation ($r = 0.32$, $p = 0.04$) between AI implementation and stakeholder confidence in ethical governance reflects persistent concerns about transparency and accountability. Participants expressed unease over opaque decision-making processes, commonly referred to as "black box" algorithms. Instances of bias in facial recognition and decision-support tools were cited as significant barriers to trust. These findings are consistent with literature advocating for participatory ethical frameworks that address algorithmic bias and ensure equitable outcomes.

**Critical Analysis of the Interviews**

The section focuses on rich qualitative data gathered through the interviews offering the critical analysis of patterns and themes emerged from strategic implementation of the AI in UAE security and defense. The findings get interpreted against backdrop for existing practical implications and theoretical framework which highlights complexities and nuances.

**Theme 1 - The Enhanced Decision-Making**

A dominant theme has been a perceived enhancement for decision making process through the AI integration. The participants have consistently emphasized ability of AI for analysis of vast datasets in the real time ensuring more informed and quick decision. It aligns with the global trends where the defense organizations would leverage AI for interpretation of satellite imagery and prediction of threats. Example – the interviewee has cited the recent incident where the predictive analytics has successfully anticipated the potential cyberattack while allowing the preemptive counter measures.

However, there are concerns emerging about reliability for AI generated insights in particular for high stake situations. A participant noted: AI could provide the accurate data but the interpretations needed the human validation across the ambiguous scenarios. The perspective highlights need for the hybrid approach which combines capabilities of AI with human expertise. The findings are resonating with the literature highlighting risks for the AI over reliance in particular when the algorithms lack the contextual understanding.

**Theme 2: Cybersecurity and the Adversarial AI**

Cybersecurity is another recurring theme with the particular highlights role of AI in mitigation and identification threats. The advanced machine learning algorithms have been proven effective for detection of anomalies like unauthorized access and phishing attack attempts. The defense strategists has explained, “The AI systems significantly reduced the response time during the cyber incidents while often neutralizing the threats before it escalates.

Despite the advancement, the adversarial AI like algorithmic exploitation and deepfakes have significant challenges. The participants have expressed the concerns over increasing sophistication of technologies which could deceive both AI systems and human operators. A interviewee cited the incident where the deepfake video had triggered a diplomatic crisis which involved the high stakes. It highlights need for adaptive AI models which are capable for countering the threats and international collaboration for developing the standardized counter measures.

**Theme 3: Autonomous Systems and the Reliability**

Autonomous system deployment includes robotic vehicles and drones which are frequently discussed. The participants are praising the technologies for improving the operational efficiency and reducing the human risks. The defense operator ensures successful surveillance mission where the drones provide the real time data across hostile environment which improves the situational awareness.

But, reliability issues are persisting. Many interviewees have highlighted instances where the autonomous systems have misidentified or malfunctioned targets further leading towards operational setbacks. The participant remarked, “Although the drones are effective, the errors can at times negate benefits the critical missions”. The findings highlight need for the robust fail safe mechanism and ongoing the human oversight for mitigation of potential risks. The literature is further supporting the view which advocates hybrid systems which integrates the

autonomous functionalities with the human decision making capabilities.

**Theme 4: Ethical Challenges and the Transparency**

Ethical considerations have emerged as the central theme with the participants voicing concerns on lack of transparency across the AI systems. Opaque nature for the black box algorithm is often hampering accountability, in particular for cases where the decision have significant consequences. The interviewee shared the scenario where the AI tool is recommending the resource allocation to be questioned for the unexplained biases.

Additionally, there are also concerns about the societal implications of the AI across defense in particular for surveillance and privacy. The participants are stressing importance for ethical framework which balances the security needs with the individual rights. Example – the policy expert is suggesting – We need the participatory framework which involves the different stakeholders for ensuring the ethical deployment of AI. It aligns with the academic calls for the co-designing of the ethical guidelines for addressing the algorithmic biases and ensuring the equitable outcomes.

**Theme 5: Training and the Skill Development**

The interviews further highlighted importance for comprehensive training programs for the defense personnel. The participants have emphasized need for the special training at interpreting AI outputs, responding to the adversarial threats and managing ethical dilemmas. The scenario based simulations are effective tools for preparing the team with actual challenges. However, there are multiple respondents who highlighted the gaps in the training programs in particular towards interdisciplinary skills. The interview remarked –"The technical proficiency is not enough alone. One needs the personnel who understands the AI algorithm and the broader implications. The insights highlight need for the training initiative which integrates the strategic, ethical and technical dilemma.

**Theme 6: International Collaboration and the Policy Development**

With global nature for the AI challenges, the participants have underscored importance for the international collaboration. It shares the best practices and development of joint counter of AI strategies have been identified as important steps. The interviewee mentioned, "Collaboration of international allies could help in staying ahead of the adversarial technologies and establishment of global ethical standards.

Policy development was another area where the interviewees discussed. The participants have advocated for the robustness in regulatory framework for governing the ethical implementation of AI. The recommendations include the mandatory algorithms for audit, penalties for non-compliance and explainability requirement. The suggestions are aligned with the global trends where the countries are increasing the prioritization of AI governance for ensuring trust and accountability.

**Theme 7: The Longitudinal Impact Assessment**

Need for the longitudinal studies for assessing the sustained impact of AI on the defense operations is an important theme. The participants argued on short term metrics to often fail at capturing long term implications for AI adoption. A strategist observed, "AI systems are evolving over the time and its effectiveness needs to be evaluated continuously for ensuring alignment with the operational goals.

The assessments could provide the valuable insights for AI evolution while identifying the

areas across informing and improving the future investments. The literature supports the perspective while emphasizing importance for ongoing evaluation for maximization of AI potential while mitigating the risks.

## Discussion

### Improved Decision-Making Capabilities

The findings highlight transformative role played by AI for improving the decision making. The survey data analysis highlights strong correlation of $r=0.78$ and $p<0.001$ between improved decision making and AI integration. The findings are aligned with the studies AI ability for processing the large data sets across real time while enabling the proactive response for the security threats (Huang & Rust, 2021). Predictive analytics used during the Expo 2023 predicted the potential threats through analysis of visitor behavior, the practical demonstration for AI impact.

But, the qualitative feedback highlights the risks for over reliance on the AI systems. The different participants have cautioned the incomplete or biased datasets can lead to flaw in decision making during the critical operations (Binns, 2018) further emphasizes such errors could have cascading effect across the defense sector where lives are important. Such as the documented failure where the AI misidentified the hospital forces during the military exercise that led to resource misallocation.

Further, significant gap has been noted for integration in contextual judgement which is important strength for the human decision makers. The interviewees frequently mentioned the situations where the AI recommendations being disregard because of the misalignment on the ground realities. It underscores necessity for hybrid decision making models which leverages the AI computational strengths while it retains the human oversight.

### Strengthened Cybersecurity

The AI contributions for cybersecurity has been prominent in findings. The moderate positive correlation $r=0.64$ and $p<0.01$ which is observed between cybersecurity improvement and AI adoption. The AI powered tools have been credited with neutralizing and identification of cyber threats which is faster than the human analysts. During the UAE government simulation in 2023, AI had successfully detected and also blocked the phishing attack which targeted the critical infrastructure in seconds.

However, the challenges which was developed in adversarial AI. The respondents have raised the concerns on increasing sophistication for the AI based cyberattacks like ransomware and deep fakes. The use of AI based deep fakes for impersonating the senior officials which bypassed the traditional security protocols. Galliott (2018) demonstrates adversarial AI has often exploited the vulnerabilities in the existing systems while making it imperative for designing the adapting defenses capable for countering the threats.

Another important insight has been lacking of the preparedness for zero-day exploits which attacks the targets of unknown vulnerabilities. While AI is excelling pattern recognition, the effectiveness is diminishing while dealing with the novel attack vectors. It underscores need for updating the AI models and continuous training for mitigating and anticipating the emerging threats.

### Operational Efficiency through the Autonomous Systems

The autonomous systems like the unmanned vehicles and drones have been identified as the

gram changers to improve the operational efficiency. The quantitative data highlighted mean score for 4.0 and SD of 0.7 for the operational efficiency which highlights consensus on role for AI to reduce the human exposure for risks. The autonomous drones implemented in UAE borders significantly improved the surveillance accuracy and also reduced the response time for security breaches.

On other hand, the qualitative insights highlight the important concerns. The participants have cited scenarios where the drones have misidentified the targets which led to the operational errors. As of 2021 case study from the neighboring regions has detailed incident where the autonomous drones have been mistakenly classified civilian vehicle as the threat which resulted in the collateral damage. The findings have aligned through literature through Sparrow 2020 who is arguing lack of the contextual awareness across AI systems leading towards operational and ethical challenges.

The maintenance of the autonomous vehicles as has developed as the recurring theme. Although AI enhances the operational efficiency, the reliance on the high-quality data and consistency in updates is making it susceptible for degrading over the period of time. The interviewees have emphasized importance for robust maintenance protocols for ensuring reliability for autonomous systems in the critical missions.

**Ethical Considerations and the Human-AI Collaboration**

Ethical considerations developed as persistent challenges while receiving lowest mean of 3.2 and SD of 0.9. Although guidelines for AI ethics exists, the interviews haven been criticized for limiting the enforcement and lack of the transparency across Al algorithms. The black box systems where the decision-making processes are the opaque where the frequency is mentioned as barrier for accountability.

The issue is critical across defense where the errors could have the life or the death consequences. The weak correlation of r=0.32 and p=0.04 between ethical confidence and AI adoption reflecting broader skepticism about ethical governance for AI systems. Cath (2019) and Galliott (2018) would argue lack of the explain ability in the AI systems undermining the trust while making it imperative for prioritizing transparency.

The literature reviews highlighted implementation of the facial recognition systems at the public surveillance which has often led to raising concerns and false positives for privacy violations. In case of UAE, although the AI systems improved the treat detection, the opacity has at times resulted in eroding the public trust, unjust profiling which includes the different stakeholders for ensuring ethical considerations are embedded from outset.

**Implications for the Theory**

The findings are contributing towards theoretical understanding for role of AI across security and defense in UAE highlighting inherent challenges and transformative potential

Advancing the Decision-Making Models – Study highlights existing theories where AI improves decision making through real time insights. However, it challenges the deterministic views for AI as the infallible further emphasizing need for the hybrid models which integrates with the human judgement.

Ethical AI framework – the study is adding the empirical weight for the calls of Ethical AI framework in particular for defense where transparency and accountability is important. It also highlights limitations for the current models, urging for shift towards the participatory design processes which includes the different stakeholders.

Dual Use of the Dilemma across Cybersecurity – Dual edge nature for AI across cybersecurity is aligned with dual use of the dilemma framework which is exploring how the technologies are designed for the protection could be weaponized.

**Implications for Practice**

The research does have the significant practical implications for the defense strategists, policy makers and the technologists

Balancing integration for Human Oversight and AI : Although AI is enhancing the operational efficiency, the over reliance has the risks. The defense organizations need to adopt for hybrid approach where the AI is supporting instead of replacing the human decision making. The training programs need to be designed for equipping personnel with skills for interpreting the AI outputs critically. Further, the human operators need to retain the ultimate decision-making authority in particular across life critical scenarios and preventing the mishaps being caused through AI misalignment.

Investment in the Counter AI strategies: With the growing adversarial of AI, the investment across counter AI technologies has been imperative. It includes development of systems which could neutralize and identify the AI driven cyberattacks and foster collaborations with the global cybersecurity experts for staying ahead in emerging threats. The strengthening of partnerships with the international defense organizations could also help the UAE for leveraging the cutting-edge counters for AI solutions while sharing the threat intelligence effectively.

Regulatory Framework in Ethical AI: In order to address the ethical concerns, the policymakers need to establish the comprehensive regulatory framework which enforces accountability and transparency. It includes the mandatory audit for the Al algorithm, requirement, explain ability and penalties for the noncompliance. The establishment of independent in AI ethics council can further strengthen the governance. Also, the regular reviews for AI systems in the defense settings is important for ensuring the compliance with the changing ethical standards and addressing the emerging challenges.

Continuous Innovation across the Autonomous Systems: In order to enhance reliability for autonomous systems, it is important to invest in the advanced machine learning. Real time feedback and context awareness for AI models could improve the accuracy across complex environment. Also, the fail-safe mechanism could integrate for allowing the human operators for intervening as required. The future innovations shall focus on development of energy efficient and light weight AI systems for improving deployment of the autonomous systems in the resource constrained or remote areas.

Public Awareness and Stakeholder Engagement: Building the trust across AI technologies need engaging stakeholders across defense ecosystem which includes civil society, policymakers and technologists. The public awareness campaigns could also help in demystifying AI, fostering informed decisions and addressing the misconceptions about the role across defense. The encouraging of public discourse on the operational and ethical implications of AI could further build the societal acceptance and trust.

Development of the Context based AI systems: The defense applications need the context aware systems in AI which could adapt towards challenges in local security. The AI solutions tailored for unique geographical landscape of UAE, defense requirement and cultural requirement could improve the efficacy significantly. The collaboration with the local

universities and research institutes could drive the innovation in the area while ensuring development of the AI systems which align with the national priorities.

Integration of the Cross Functional Expertise: AI across the defense in the multi-disciplinary challenges needs expertise from the fields like ethics, data science, policy and engineering. Encouraging of collaboration among the domains could ensure the holistic approach towards AI deployment and development. The interdisciplinary task force could oversee design, monitor and implement the AI systems while balancing the technical innovation with the operational and ethical considerations.

## REFERENCES

Ahmed, Alfaki, A. a., C M, I. (2013). Transforming the United Arab Emirates into a knowledge-based economy: The role of science, technology and innovation. *World Journal of Science, Technology and Sustainable Development*, 84--102.

Al Zarooni, A. A., Prinsloo, S. H., Nagelkerke, E. A., C Nico. (2019). Prevalence of vitamin D deficiency and associated comorbidities among Abu Dhabi Emirates population. *BMC research notes*, 1--6.

Al-Ammal, Aljawder, H. a., C Maan. (2021). *Strategy for artificial intelligence in Bahrain: Challenges and opportunities*. Springer. al-Assad, B. (2000). Bashar al-Assad. *change*, 21.

Almahri, G. a., Shehadeh, Y. a., ElHassan, K. a., Ahmed, A. a., Alzahmi, W. a., C Salem. (2023). *Characterization of Hybrid FRP Composite Produced from Recycled PET and CFRP*. MDPI.

Almansoori, Al-Emran, A. a., Shaalan, M. a., C Khaled. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences*, 5700.

Alneyadi, Hamid, R. H., C Abdul, N. A. (2021). Hierarchical Order of User Preference Parameters in Adopting M-government Services. *International Journal of Sustainable Construction Engineering and Technology*, 219--231.

Alneyadi, Hamid, R. H., C Abdul, N. A. (2021). Hierarchical Order of User Preference Parameters in Adopting M-government Services. *International Journal of Sustainable Construction Engineering and Technology*, 219--231.

Alnuaimi, C Mouza. (n.d.). Analyzing the current relationship between the UAE and China: Strategic Hedging or Diversification of Partners?

Al-Suqri, Gillani, M. N., C Maryam. (2022). A comparative analysis of information and artificial intelligence toward national security. *IEEE Access*, 64420--64434.

Al-Suqri, M. N., C Gillani, M. (2022). A comparative analysis of information and artificial intelligence toward national security. *IEEE Access*.

Awad, Al-Shaye, A. a., C Dana. (2014). *Public awareness, patterns of use and attitudes toward natural health products in Kuwait: a cross-sectional survey*. Springer.

Bachmann, Bell, J. a., Holmqvist, C. a., C Caroline. (2015). *War, police and assemblages of intervention*. Routledge London.

Bernard, C Russell, H. (1996). Qualitative data, quantitative analysis. *CAM Journal*, 9--11.

Bertossi, Marangon, A. a., Troiano, F. a., C others, S. a. (2023). Assessment of the Sustainable Level of Vending Machine Products in an Italian University. *The International Journal of Environmental Sustainability*, 19.

Chandra, Sharma, G. R., Liaqat, B. K., C Ali, I. (2019). UAE's strategy towards most cyber resilient nation. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 2803--2809.

Cowan, C Glen. (1998). *Statistical data analysis*. Oxford university press.

El-Kebbi, Bidikian, I. M., Hneiny, N. H., Nasrallah, L. a., C Philippe, M. (2021). Epidemiology of type 2 diabetes in the Middle East and North Africa: Challenges and call for action. *World journal of diabetes*, 1401.

Fonseca, L. a., Malinowski, G. a., Mari, F. a., Gadelha, J. a., C Ary. (2020). Schizophrenia and COVID- 19: risks and recommendations. *Brazilian Journal of Psychiatry*, 236--238.

Franzosi, C Roberto. (2010). *Quantitative narrative analysis.* Sage.

Hughes, E. a. (2018). Unlocking blockchain: Embracing new technologies to drive efficiency and empower the citizen. *The Journal of The British Blockchain Association*, 2.

Jamil, M. a. (2016). Renewable energy technologies adopted by the UAE: Prospects and challenges--A comprehensive overview. *Renewable and Sustainable Energy Reviews*, 1181--1194.

LeCompte, C D, M. (2000). Analyzing qualitative data. *Theory into practice*, 146--154.

Mearsheimer, C J, J. (2021). The inevitable rivalry: America, China, and the tragedy of great-power politics. Foreign Aff, 48.

Mearsheimer, J. J. (2001). *The tragedy of great power politics.* WW Norton \C Company.

Mobra, Hamlin, T. a., C Daniel. (2020). Emergency Certified Teachers' Motivations for Entering the Teaching Profession: Evidence from Oklahoma. *Education Policy Analysis Archives*, n109.

Neyadi, A., Blooshi, S. S., Nguyen, A. G., Alnaqbi, H. L., C A, M. (2021). UiO-66-NH 2 as an effective solid support for quinazoline derivatives for antibacterial agents against Gram-negative bacteria. *New Journal of Chemistry*, 20386--20395.

Robertson, Kim, A. G., Al-Ahmadie, J. a., Bellmunt, H. a., Guo, J. a., Cherniack, G. a., . . . others, R. a. (2017). Comprehensive molecular characterization of muscle-invasive bladder cancer. Elsevier.

Sayler, C M, K. (2020). Artificial intelligence and national security. *Congressional Research Service*, 45178.

Seers, C Kate. (2012). Qualitative data analysis. *Evidence-based nursing*, 2--2.

Shdefat, A., Awar, S. a., Osman, S. a., Khair, N. a., Sallam, H. a., Maki, G. a., C others, S. a. (2022). Identification level of awareness and knowledge of Emirati men about HPV. *Journal of Healthcare Engineering*, Hindawi.

Sheard, C Judithe. (2018). *Quantitative data analysis.* Elsevier.

Smith, Davies, K. a., C Joanne. (2010). Qualitative data analysis. *Practical researcher and evaluation: A start-to finish guide for practitioners*, 145--158.

Szalai, M. (2021). *The foreign policy of smaller Gulf States: size, power, and regime stability in the Middle East.* Routledge.

Waltz, C N, K. (1993). The emerging structure of international politics. *International security*, 44--79. Waltz, C N, K. (2010). *Theory of international politics.* Waveland Press.

Weissmann, Nilsson, M. a., Palmertz, N. a., Thunholm, B. a., C Per. (2021). *Hybrid warfare: Security and asymmetric conffict in international relations.* Bloomsbury Academic.

Yaacoub, Noura, J.-P. A., Salman, H. N., Chehab, O. a., C Ali. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, 115--158.

Zaabi, A., Zamri, S. H., C Ruzaidi. (2022). Managing security threats through touchless security technologies: An overview of the integration of facial recognition technology in the UAE oil and gas industry. *Sustainability*, 14915.