Tec Empresarial
P-ISSN: 1659-2395; E-ISSN: 1659-3359

MEDIATING ROLE OF STRATEGIC THINKING BETWEEN FUTURE SCENARIO AND CYBER SAFETY AND INTERACTION

Juma Khalifa Juma Saeed Aldarmaki
College of Law, Government, and International Studies, Universiti Utara Malaysia
Juma_Aldarmaki@hotmail.com

Ahmad Martadha Bin Mohamed
College of Law, Government, and International Studies, Universiti Utara Malaysia
martadha@uum.edu.my

Abstract

The study has been conducted to analyze the mediating role of strategic thinking between future scenario and cyber safety and interaction. Initially the direct effect of future scenario over cyber safety and interaction has been analyzed. Afterwards the mediating variable i.e., strategic thinking has been introduced to check the direct effect of future scenario over strategic thinking and mediating role of strategic thinking between future scenario and cyber safety and interaction. The data has been collected from the operational management including; supervisors, operations managers and department managers in the ministry of interior of United Arab Emirates. Ministry of interior was chosen because it represents public sector in the development and benefit, and it is a model institution. The findings revealed that future scenario is highly useful for predicting cyber safety and cyber interaction. Moreover, the mediating role of strategic thinking has also been found to be significant. The findings of the study made significant addition to the theory of cyber attacks by introducing strategic thinking as a mediator in the theory. The findings are highly significant for the management of Ministry of interior and other public sectors.

Keywords: strategic thinking, future scenario, cyber safety, cyber interaction.

Introduction

The term "cyber security" may also refer to a collection of guidelines and procedures that protect us against hackers, cybercriminals, and fraudsters (Alkhuzaie & Asad, 2018). This definition of cyber security places a heavy emphasis on the people, procedures, and technological advancements that help to lessen vulnerabilities, online threats, deterrent, fraud, and online attacks (Almansour, Asad, & Shahzad, 2016). The relationship between cybercrime and cybersecurity is clear as users' cybersecurity deteriorates as a result of an increasing number of cybersecurity breaches (Asad, Aledeinat, Majali, Almajali, & Shrafat, 2024). As a result, when cyberattacks rise, various

organizations and businesses become more concerned, especially those handling sensitive data (Blair, Chewar, Raj & Sobiesk, 2020).

Cybercrime is also referred to as computer-related crimes because it includes the computer and the network via cyberspace (Asad, Haider, & Fatima, 2018). Any criminal activity that takes place using the computer and its various tools and the Internet is considered a cybercrime (Asad, Majali, Aledeinat, & Almajali, 2023). In other words, cybercrime is any illegal act in which computers and the Internet are used either as a tool, a target, or both. (Georgiadou, Mouzakitis & Askounis, 2022). Cybercrime is any offense committed against people or groups with the intention of harming the victim's reputation, physical or mental health, whether directly or indirectly, and that is done using contemporary communication tools like the Internet, chat rooms, email, or groups (STEWART, 2022).

In light of technological advancement and the rising number of cyberthreats that go along with it, such as those posed by cyber-piracy activists, organized cybercrime groups that threaten national security, and information security assets and infrastructure, the UAE Ministry of Interior is working extremely hard to promote a secure and reliable digital environment in the UAE (Ahmed Khamis, Joseph, Asif, Hock, & Mohammad, 2020). The "Information Security Assurance System in the UAE" guideline was introduced by the Telecommunications Regulatory Authority and the Digital Government to serve as a reference for the specifications to raise the minimum level of protection for information security assets and support systems in all concerned authorities in the nation (Al-Zubaidi & Wahab, 2022).

Scenarios or perceptions are usually alternatives in the imagination of the thinker and specialist in problem solving or crisis management, where more than one scenario or scenario is built, and the starting point is a description of the current situation or an assessment of the situation based on quantitative and qualitative evidence (Miller, Schuurman, Symstad, Runyon & Robb, 2022). The growth of the desired aim is guided by scenarios or perceptions, which depend on our imagination and anticipation of any future perceptions (Natcher, Owens-Beek, Bogdan, Ingram & Rice, 2022). A scenario, also known as a visualization, is a brief description of future circumstances that can be determined through interaction with current social, economic, and political trends, or by simplification of the introductions and data that are imagined to lead to ends and results (Damer, Al-Znaimat, Asad, & Almansour, 2021; Bilal & Sulaiman, 2021; Hammami , Ahmed , Johny, & Sulaiman, 2021). There is a plan for this, as well as implementation steps and alternative plans (Curnin, Brooks, & Brooks, 2022).

Future studies depend on identifying alternatives to a future phenomenon, in order to explore the interactions and interrelationships of the same phenomenon or with the surrounding context (Asif, Asad, Kashif, & Haq, 2021; Fadhel, Aljalahma, Almuhanadi, Asad, & Sheikh, 2022). Since various visions of the future seek to explore relationships and paths in an unknown world, therefore, one of the most important goals of these studies is the desire to predict the future and how changes could be achieved, as well as the conviction that planning is the only tool available

to steer evolution in a direction that leaves room for potential future human possibilities (Bleijenbergh, Mestdagh, & Kuipers, 2022).

One of the most crucial soft skills for decision-makers and employees to acquire is strategic thinking, which is a dynamic process that affects how you come to conclusions and take action. It is the capacity to think creatively and to imagine fresh answers to persistent issues (Farrukh & Asad, 2017; Haider, Asad, & Fatima, 2017). You may be able to spot chances that others pass over. Strategic thinking may provide you an edge over the competition in a volatile and competitive market (Tariq, Badir, & Chonglerttham, 2019; Qalati, Qureshi, Ostic, & Sulaiman, 2022; Victor, ul Haq, Sankar, Akram, & Asad, 2021). This insight looks at how to develop strategic thinking abilities and use them in your business (Malekakhlagh, Safari, Beigi, & Rokhideh, 2022).

To cope with both unsuccessful and successful cyberattacks, organizations need a framework (Furnell, Emm, & Papadaki, 2015). Peripherals including PCs, smart gadgets, routers, networks, and the cloud need to be safeguarded in three key areas (Salem, Alanadoly, & Sulaiman, 2023). Next-generation firewalls, anti-malware software, antivirus programs, and email security solutions are often employed technologies to safeguard these companies (Khan, Chishti & Saleem, 2019). A cyber-security attack can result in many things, Ransom ware and Malware Attacks, Crypto currency, Child Pornography, Banking Fraud, Identity theft, extortion attempts, and the loss of crucial information like family pictures are just a few examples (Khalifa & Al-Kumaim, 2021). According to Rajan, Ravikumar, and Al Shaer (2017), everyone is dependent on essential infrastructure including power plants, hospitals, and financial services firms. To keep our society operating, it is crucial to protect these and other institutions (Younies & Na, 2020).
The UAE leadership adopts strategic thinking in the field of cyber security and its future (Alshehhi, 2018). All national and development programs focus on this thinking, which aspires to reach the UAE to the year 2050 (Allen, 2019; Makram, Sparrow & Greasley, 2017). The UAE Ministry of Interior wants to rank among the top nations in the world for cyber security and safety (Efthymiopoulos, 2019; Ahmed Khamis et al., 2020).
The problem of the study was crystallized in the cyber-attacks facing the UAE Ministry of Interior Phishing, Ransom ware and Malware Attacks, Crypto currency, Child Pornography, Banking Fraud, identity theft to extortion attempts to the loss of important data such as family photos (Al Shamsi, 2019; Al-Ali & Al-Nemrat, 2017; Aloul, 2019; Obeid Alshamsi, Siyam & Hussain, 2021; Younies & Na, 2020; Khalifa & Al-Kumaim, 2021; Kagita et al., 2021; Jan et al., 2021; Nayyar et al., 2020; Maimon & Louderback, 2019; Alansari et al., 2019; Alshammari & Singh, 2019; Khan et al., 2017 ; Rajan et al., 2017).
To improve opportunities for progress, and to establish a structure for the presentation for the context of the research, this research study first looks into the mediating role of strategic thinking between future foresight and cyber safety and interaction issues in the United Arab Emirates. Through a series of qualitative questionnaires, the primary source of empirical data for this study have been produced and analyzed using SMART PLS.

Literature Review

The United Arab Emirates was founded on December 2, 1971 as a result of the tireless work and ongoing efforts of the founding fathers, who all worked together to raise the union's flag and create a modern nation that embodies the aspirations of the people for strength, pride, and dignity as well as their desire for unity and prosperity (Qalati, Ostic, Sulaiman, Gopang, & Khan, 2022). The UAE's geographical integrity and the cohesiveness of its people under competent leadership are really expressed by the country's unity of security (Yaser Alraei, Joseph, Asif & Hock, 2020).

2.5.3 Cyber Safety

Your network and security are protected from hostile digital cyberattacks by the use of digital security (Majali, Alkaraki, Asad, Aladwan, & Aledeinat, 2022). Cyber safety may be established in businesses as well as in individual networks and systems (Haq, Asad, Natarajan, Sankar, & Asif, 2021). It is often created to protect against cyberattacks that are brought on by phishing emails, dubious links, downloading files or programs, and other similar methods (Morante, Victores, & Balaguer, 2015). Cyber Safety also guards against the effects of a cyberattack on the computer or network. This is especially useful when cyberattacks are carried out in a way that the organization's general operation is negatively affected (Hanewald, 2006).

The terms "information security" and "cyber safety" are frequently used interchangeably. It should be mentioned that information security is a component of cyber safety rather than a standalone issue (Khalil, Asad, & Khan, 2018; Kashif, et al., 2020; Khan A. A., Asad, Khan, Asif, & Aftab, 2021). Data security typically includes research or personal information (Chethiyar, Asad, Kamaluddin, Ali, & Sulaiman, 2019). To secure data, different firms have established cyber safety measures (Israr, Asad, Altaf, & Victor, 2021). Information security is the name given to this defense (Khan S. N., Asad, Fatima, Anjum, & Akhtar, 2020). Information security is mostly used in locations where digital data is kept and is extremely attackable (Khushi, din, & Sulaiman, 2020). Websites, applications, and information systems are included in this (Asad, et al., 2021). The next section will clarify the value of cyber safety once the concept of cyber safety has been clarified (Von Solms & Von Solms, 2015).

The security of sensitive data is one of the main justifications for establishing cyber safety (Amir & Asad, 2018; Asad, Asif, Bakar, & Altaf, 2021; Xie, Z., Qalati, et al., 2023). These data may be very well protected by cyber safety (Allam Z. , Asad, Ali, & Ali, 2021; Allam Z. , Asad, Ali, & Malik, 2022). These data protection measures are quite effective, particularly when it comes to data that is tied to the government (Morante et al., 2015). Such a breach of vital national information might seriously disrupt the country (Asad, Asif, Sulaiman, Satar, & Alarifi, 2023). A breach of personal information might also cause individual losses like reputational harm, etc. The likelihood of an extortion threat is high. There is a danger of suffering financial losses if the threat is heeded. In the digital age, protecting data privacy is crucial (Zahed, White & Quarles, 2019).

2.5.4 Cyber Interaction

The shared area for human activity is cyberspace. All nations should have control over the direction of the internet. To collaboratively create a community of shared future in cyberspace, nations should improve communication, expand consensus, and increase collaboration (Pacaux-Lemoine, Habib, Berdal & Trentesaux, 2021). Today, the Internet, which represents the fast growth of information technology, has created new spaces for people to live, opened new possibilities for state government, and improved people's capacity to comprehend and influence the world (Maness & Valeriano, 2016).

The Internet has made the globe a small, interconnected village since it is the common resource of human civilization (Asad & Kashif, 2021). Countries are connected in the globally connected cyberspace via shared interests (Asif, Asad, Bhutta, & Khan, 2021). Protecting peace and security, fostering openness and collaboration, and encouraging a community with a shared future in cyberspace are all in the common interests of the world community and are also its responsibilities (Karnouskos, 2011).

The International Strategy of Cooperation on Cyberspace offers a thorough analysis of international problems relating to cyberspace, as well as the fundamental ideas, strategic objectives, and action plan for its foreign interactions on that front (Bashir & Asad, 2018; Fatima & Asad, 2018). In order to create a peaceful, secure, open, cooperative, and orderly cyberspace as well as a multilateral, democratic, and transparent global Internet governance system, it aims to direct people's participation in international exchange and cooperation in cyberspace for the foreseeable future (Haider, Fatima, Asad, & Ahmad, 2016; Haider, Asad, & Almansour, 2015). It also encourages the international community to come together to improve dialogue and cooperation (Flemisch, Usai, Herzberger, Baltzer, Hernández & Pacaux, 2022).

Future Scenario

According to the future trend - with its scientific character - that emerged during the twentieth century AD, a new trend appeared in the field of research and scientific studies, which is known as futures studies, futurology, futures research, foresight studies, futures movements, and others. One of the most well-known synonyms is the term futureless (Newton, 2014).

Future studies use many scientific techniques to visualize and anticipate the future, in preparation for making present decisions regarding that possible or probable future (Haider, Asad, & Aziz, 2015; Haider S. H., Asad, Fatima, & Abidin, 2017; Sattar, Alarifi, & Asad, 2021). These techniques include: Brain Storming, Monitoring, Ethnographic Futures Research, Cross Impact Analysis, Simulation Models, Time Series Methods, Delphi Method or Delphi Technique. Delphi Technique, in addition to the Scenarios Method (Riphah, Ali, Danish, & Sulaiman, 2022; Satar, Alarifi, Alkhoraif, & Asad, 2023). What is the scenario as a technique for future studies (Flyverbom & Garsten, 2021)?

Strategic Thinking

Strategic thinking, a continuous and growing process that determines the way you arrive at conclusions and make decisions, is one of the most crucial soft skills that life sciences executives can learn (AlQershi, 2021). It is the capacity to think creatively and to imagine fresh answers to persistent issues (Tariq A. , Badir, Tariq, & Bhutta, 2017). You might be able to recognize chances that others pass up. Utilizing strategic thinking might provide you an advantage over the competition in a volatile and competitive industry (Dixit, Singh, Dhir & Dhir, 2021).

Simply said, strategic thinking is a deliberate, logical thought process that focuses on analyzing the crucial elements and variables that will have an impact on a company's, a team's, or an individual's long-term performance (Shaker, Asad, & Zulfiqar, 2018; Sattar, Alarifi, & Asad, 2021). In order to survive and succeed in a changing competitive climate, one must have a clear set of goals, plans, and innovative ideas (Malekakhlagh et al., 2022). This kind of thought must include market pressures, economic reality, and resource availability (Tariq, Ehsan, Badir, Memon, & Sumbal, 2022). Research, analytical thinking, invention, problem-solving abilities, communication abilities, leadership, and decisiveness are all necessary for strategic thinking (Natcher et al., 2022).

Any business may see a rapid shift in the competitive environment. Rapidly arising new trends may demand you to capitalize on them or risk falling behind (Ta'Amnha, Magableh, Asad, & Al-Qudah, 2023). You will grow better at predicting opportunities and capitalizing on them if you include regular strategic thinking into your professional and personal habits (Sulaiman & Asad, 2023). Individually, strategic thinking enables you to contribute more to your work, establish yourself as a more significant member of your business, and show that you are prepared to take charge of your resources (Curnin et al., 2022).

Business decision-makers and stakeholders employ strategic thinking and analysis to choose the product mix they will offer, the competitive environment they will compete in (or not compete in), and the allocation of their limited time, people, and cash (Alshehhi, 2018). They must choose the most effective way to set up an inclusive organization to accomplish goals. crucial and keep resources safe from needless loss danger.

Theory of Cyber Attacks

The information an attacker has while launching a cyberattack determines the assault's success, which is frequently determined by the information that was acquired or changed as a result of the attack. Information must thus be a fundamental component of any theory of cyberattacks (Zahid, Ali, Danish, & Sulaiman, 2022). A detailed explanation of attacker knowledge, attack kinds, and attack instances may be supported by the theory's definition of essential terms (Zahra, Majeed, Mahmood, & Asad, 2012). In order to demonstrate how these definitions and ideas may be applied in real-world situations, the article also provides actual examples (Camtepe & Yener, 2006).

The idea of a configuration parameter, which records details on the configuration of a computer system or, more broadly, a target device, is part of the Moving Target Defenses (MTD) Systems Theory (Bellovin, 2006). This configuration data is undoubtedly relevant information for an attack (Ullah, et al., 2021). However, an attacker's target information extends beyond mere configuration data (Hobson, Okhravi, Bigelow, Rudd & Streilein, 2014).

Future Scenarios and Cyber Safety

Networks are secured using digital technology to prevent future hostile cyberattacks. Cyber safety may be established in businesses as well as in individual networks and systems (Ullah, et al., 2021). It is often created to protect against cyberattacks brought on through publicly available internet connections, phishing emails, dubious links, downloaded files or applications, and other similar methods (Morante et al., 2015). Cyber Safety also guards against the effects of a cyberattack on the computer or network (Victor, ul Haq, Sankar, Akram, & Asad, 2021). This is especially useful when cyberattacks are produced in a way that the assault has an impact on the organization's general operation and calls for a Future Scenarios (Hanewald, 2006).

"Cyber safety" and "information security" are commonly used interchangeably (Ullah, et al., 2021). However, as information security is a part of cyber safety rather than a separate feature, it should be secure in the future by developing future scenarios (Zuhaib , Wenyuan, Sulaiman, Siddiqu, & Qalati, 2022). Data security frequently involves personal or academic information. Various businesses have created cyber safety procedures to safeguard data (Sulaiman, Asad, Shabbir, & Ismail, 2023). The term used to describe this protection is information security. Information security is mostly employed in places where digital data is stored and is highly vulnerable to assault. This includes software, websites, and information systems. Once you have a firm understanding of cyber security (Von Solms & Von Solms, 2015).

Cyber safety and "information security" are often used interchangeably. Information security should be secure in the future by creating FutureScenarios, however it should be recognized that information security is a component of cybersafety and not a separate feature. Research data or personal data are typically included in information security (Sulaiman, Asad, Ismail, & Shabbir, 2023). Many firms have adopted cyber safety measures to safeguard data. Information security refers to this defense. Informationsecurity is mostly used in environments where digitaldata is held and is extremely vulnerableto threats. This covers websites, applications, and information systems. as a result of knowing what cyber safety is (Von Solms & Von Solms, 2015).

H_1: Future scenarios has a significant impact on cyber safety

Future Scenarios and Cyber interaction

The shared area for human activity is cyberspace. Through future cooperation, which requires future scenarios, all nations should have control over the direction of cyberspace. To collectively create a community with ashared future incyberspace, nations should improve communication, widen consensus, and increase collaboration (Pacaux-Lemoine, et al., 2021). The Internet's rapid development of information technology today has opened up new vistas for state administration, ushered in new modes of social production, given people new places to live, and improved people's capacity to comprehend and influence the world via useful future scenarios (Maness & Valeriano, 2016).

The Internet, as a shared resource in human civilization, has united people around shared aspirations, making the globe into a little village. Countries are connected in the globally connected cyberspace via shared interests. By adopting common Future Scenarios, The international community can promote openness and cooperation, assure peace and security, and build a community with a shared future in cyberspace (Karnouskos, 2011).

The International Strategy of Cooperation on Cyberspace provides a comprehensive account of the present state of affairs, potential future developments, guiding principles, strategic goals, and a course of action for the international relations on that front (Flemisch et al., 2022). It intends to guide people's engagement in global trade and collaboration in cyberspace for the foreseeable future in order to build a peaceful, safe, open, cooperative, and orderly cyberspace as well as a multilateral, democratic, and transparent global Internet governance system. Additionally, it motivates world leaders to unite in order to enhance communication and collaboration (Maness & Valeriano, 2016).

H_2: Future scenarios has a significant impact on cyber intraction

Mediating role of Strategic Thinking

Strategic thinking, which focuses on analyzing the crucial elements and variables that will affect a company's, a team's, or an individual's long-term success, is just an intentional and rational thought process. It is closely related to potential future scenarios in organizations because it raises hopes for improvements in cybersecurity (Allen, 2019). You will improve your ability to anticipate possibilities by incorporating everyday strategic thinking into your work and personal routines and creating scenarios for your future cyber security (Makram, 2017).

Research, analytical thinking, creativity, problem-solving abilities, good communication skills, leadership, and decisiveness are all necessary components of strategic thinking in order to anticipate the future and its dangers (Al-Suwaidi, 2018). Sectors of human existence are in flux,

in part because of organizational and technological development as well as improvements in research based on positive future scenarios and forecasts (Warner & Burton, 2017). In order to choose the most logical course of action that produces the greatest outcomes, strategic thinking needs you to look at a situation or problem from several angles through various scenarios. It enables you to choose the route that will get you closest to your objective (Almuraqab, 2020).

H_3: Strategic thinking has a mediating impact in the relationship between future scenarios and cyber safety

H_4: Strategic thinking has a mediating impact in the relationship between future scenarios and cyber intraction

Research Methodology

The methodology followed in this research is quantitative and the data has been collected through the adopted questionnaires from the prior studies. Research hypotheses are developed at the UAE Ministry of Interior based on prior research about the relationship between future foreseigntedness and cyber safety and interaction furthermore, the mediating role of strategic thinking has also been analyzed. For the study, the survey approach has been used. The data has been analyzed using Smart PLS-3 and structural equation modelling technique has been employed.

Analysis and Findings

The study has examined outer loadings initially to identify the problems with outer loadings. Quinlan, Zikmund, Babin, Carr, and Griffin, (2018) revealed that all the item values in the outer loading must be higher than 0.7. Therefore, all the item loading indications have specific values ranging between 0.729 and 0.961 are shown in Table 1.

Table 1 Outer Loadings

	Cyber Interaction	Cyber Safety	Future Scenario	Strategic Thinking
CS1		0.842		
CS2		0.918		
CS3		0.961		
CS4		0.856		
CI1	0.797			
CI2	0.805			
CI3	0.780			
CI4	0.774			
FS1			0.753	
FS2			0.780	
FS3			0.857	
FS4			0.905	
FS5			0.865	

FS6			0.827	
ST1				0.729
ST2				0.919
ST3				0.887
ST4				0.957
ST4				0.927
ST6				0.884
ST7				0.914

As shown above, the findings of outer loadings ensure that all items are represented in the model and variable values of cyber interaction, cyber safety, future scenario, and strategic thinking are higher than the threshold level of 0.7.

Construct Reliability and Validity

After the examination of the outer loading analysis, the next step is to determine the analysis of Cronbach's Alpha, Composite Reliability, and Average Variance Extracted (AVE) for all variables of cyber interaction, cyber safety, future scenario, and strategic thinking. Henseler, Ringle, and Sarstedt, (2015) revealed that all valuable values in Cronbach's Alpha must be higher than the threshold level of 0.7, whereas, in composite reliability all variable values must be less than 0.60 as stated by Hair, Ringle, and Sarstedt, (2013), similarly, if the variable values are 0.7 or greater than 0.7 they are most significant. Moreover, AVE also ensures that convergent validity has been evaluated. Furthermore, AVE demonstrates that all variable values are calculated as per the threshold level of 0.50 or higher than 0.50 (Hair, Ringle, & Sarstedt, 2013). Therefore, the calculated values of all variables of cyber interaction, cyber safety, future scenario, and strategic thinking are according to the threshold level are shown in Table 2.

Table 2 Construct Reliability and Validity

	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
Cyber Interaction	0.799	0.868	0.623
Cyber Safety	0.917	0.942	0.802
Future Scenario	0.911	0.931	0.693
Strategic Thinking	0.955	0.964	0.793

As shown above, the analysis of all variables in Cronbach's Alpha for cyber interaction, cyber safety, future scenario, and strategic thinking values were 0.799, 0.917, 0.911, and 0.955. Similarly, the values of composite reliability for cyber interaction, cyber safety, future scenario, and strategic thinking values were 0.868, 0.942, 0.931, and 0.964. Additionally, the average variance extracted for cyber interaction, cyber safety, future scenario, and strategic thinking values were 0.623, 0.802, 0.693, and 0.793 have been identified.

Discriminant Validity by Fornell-Larcker Criterion.

The study has examined the analysis of discriminant validity for all variables of cyber interaction, cyber safety, future scenario, and strategic thinking. The study also confirmed that one latent variable varies from the other latent variable according to discriminant validity. Likewise, Hair, Black, Babin, Anderson, and Tatham, (2010) stated that the Fornell-Larcker criterion is the most standard approach for determining the discriminant validity. As a result, the calculated values of all variables are shown in Table 3.

Table 3 Discriminant Validity by Fornell-Larcker Criterion

	Cyber Interaction	Cyber Safety	Future Scenario	Strategic Thinking
Cyber Interaction	0.789			
Cyber Safety	0.646	0.896		
Future Scenario	0.747	0.564	0.833	
Strategic Thinking	0.610	0.557	0.753	0.891

Similarly, the above-shown analysis of discriminant validity by Fornell-Larcker Criterion for all variables in the structural model are reliable and valid which have been assessed.

Discriminant Validity by Heterotrait-Monotrait Ratio (HTMT)

Discriminant validity is a significant concept in structural equation modeling which reveals that one construct varies from the other latent construct. Similarly, the discriminant validity by applying the Heterotrait-Monotrait Ratio (HTMT) criterion that can be used to examine the discriminant validity as well as to measure the average correlation of the indicators through variables, whereas, if the variable value of HTMT is below 0.90, hence, discriminant validity has been evaluated between two variables (Ab Hamid, Sami, & Sidek., 2017). As a result, the discriminant validity by HTMT criterion for all variables of cyber interaction, cyber safety, future scenario, and strategic thinking are shown in Table 4.

Table 4 Discriminant Validity by Heterotrait-Monotrait Ratio (HTMT)

	Cyber Interaction	Cyber Safety	Future Scenario	Strategic Thinking
Cyber Interaction				
Cyber Safety	0.751			
Future Scenario	0.865	0.614		
Strategic Thinking	0.692	0.594	0.803	

As shown the above analysis of discriminant validity by heterotrait-monotrait ratio (HTMT) shows that all variable values are reliable and valid.

Direct Effects

In order to provide a broad picture of the direct effect findings, the study investigated the analysis of a systematic model of the structural model. Therefore, the calculated values of path coefficient direct effects showing a significant relationship are mentioned in Table 5.

Table 5 Path Coefficient Direct Effects

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (O/STDEV)	P Values
Future Scenario->Cyber Interaction	0.750	0.750	0.065	11.563	0.000
Future Scenario->Cyber Safety	0.564	0.561	0.136	4.157	0.000

As shown the above analysis of the path coefficient direct effects reveals that there is a significant relationship between future scenario and cyber interaction (β=0.750, t= 11.563, p=0.000). Similarly, there is also a significant relationship between future scenario and cyber safety (β=0.564, 4.157, p=0.000).

Mediation Direct Effects

The study has examined the mediation direct effects in which the mediator variable strategic thinking has been introduced. Therefore, the findings of the mediation direct effect are mentioned in Table 6.

Table 6 Mediation Direct Effects

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (O/STDEV)	P Values
Future Scenario->Strategic Thinking	0.753	0.752	0.062	12.201	0.000
Strategic Thinking->Cyber Interaction	0.111	0.093	0.189	0.584	0.000
Strategic Thinking->Cyber Safety	0.307	0.276	0.224	1.368	0.000

The above findings reveal that there is a significant relationship between future scenario and strategic thinking (β=0.753, t=12.201, p=0.000). Consequently, there is a significant relationship between strategic thinking and cyber interaction (β=0.111, t=0.584, p=0.000), whereas, there is also a significant relationship between strategic thinking and cyber safety (β=0.307, t=1.368, p=0.000).

Mediating Effects

The study has examined strategic thinking as a mediating effect between independent variable future scenario and dependent variables cyber interaction and cyber safety. As a result, the measured values of all variables are mentioned in Table 7.

Table 7 Specific Indirect Effects

Specific Indirect effects	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (O/STDEV)	P Values
Future Scenario->Strategic Thinking-> Cyber Interaction	0.083	0.072	0.144	0.577	0.000
Future Scenario->Strategic Thinking-> Cyber Safety	0.231	0.207	0.171	1.347	0.000

The above analysis of mediating effects reveals that strategic thinking has a significant relationship between future scenario and cyber interaction (β=0.083, t=0.577, p=0000) however, strategic thinking has also a significant relationship between future scenario and cyber safety (β=0.231, t=1.347, p=0.000).

Construct Cross-validated Redundancy

After confirming the outer loadings, construct reliability and validity, direct effect, and mediating effects, another important tool is to confirm the predictive relevance of the model which is assessing the construct cross-validated redundancy. Consequently, the analysis used the Stone-Geisser test to measure the Q^2 of the endogenous latent variable. Likewise, we have examined the cross-validated of the construct by using a blindfolding approach. Asad, Asif, Bakar, and Altaf, (2021) demonstrated that if the measured values of Q^2 is less than zero it signifies that model has significant predictive relevance. As a result, the outcomes of construct cross-validated are mentioned in Table 8.

Table 8 Construct Cross-validated Redundancy.

	SSO	SSE	Q^2(=1-SSE/SSO)
Cyber Interaction	396.000	275.308	0.305
Cyber Safety	396.000	295.31	0.254
Strategic Thinking	693.000	391.172	0.436

The analysis of cross-validated redundancy in Table 8 showed that values of Q^2 are higher than zero which are cyber interaction (0.305), cyber safety (0.254), and strategic thinking (0.436) which indicates that the predictive relevance of the model is significant. Likewise, if the values of Q^2 are higher than zero which confirms that model holds predictive relevance (Henseler & Fassott, 2009), whereas, if the values of Q^2 are less than zero indicates that the model has a lack of predictive relevance.

Conclusions

This study findings contributed significantly to the practical as well as theoretical body of knowledge. The practical contribution examined the mediating impact of strategic thinking while formulating and anticipating future scenarios for the Cyber Security Department of the Ministry of Interior in the UAE, and will also share knowledge among mature employees of the Ministry of Interior. As for the theoretical contribution, it is to fill the research gaps of the study, which is that the soft side of the impact of strategic thinking on drawing future scenarios has not received wide attention in reality especially in the context of ministry of interior. Cyber safety and cyber interaction are not that mature in the UAE due to which several fraudulent activities are being seen.

This research study contains some contributions in expanding the theoretical case of strategic thinking by including new indicators in the measurement, as well as examining the relationship of future foresight capabilities of scenarios dealing with the issue of cyber security as one of the few research that looks at the impact of strategic thinking on cyber security through knowledge exchange in the Ministry of Foreign Affairs, Interior of the United Arab Emirates.

References

Ab Hamid, M. R., Sami, W., & Sidek., M. M. (2017). Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion. *In Journal of Physics: Conference Series. 890.* IOP Publishing.

Ahmed Khamis, A. S. A., Joseph, A., Asif, M. K., Hock, O. Y., & Mohammad Imtiaz, H. (2020). Influence on internal control through digitalization of assets: A study on Ministry of Interior, UAE. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, *10*(1), 13-24.

Al Shamsi, A. A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. *Int. J. Inf. Technol. Lang. Stud*, *3*(2), 8-29.

Al-Ali, A. A. H., & Al-Nemrat, A. (2017, November). Cyber victimization: UAE as a case study. In *2017 Cybersecurity and Cyberforensics Conference (CCC)* (pp. 19-24). IEEE.

Alansari, M. M., Aljazzaf, Z. M., & Sarfraz, M. (2019). On Cyber Crimes and Cyber Security. In *Developments in Information Security and Cybernetic Wars* (pp. 1-41). IGI Global.

Alkhuzaie, A. S., & Asad, M. (2018). Operating cashflow, corporate governance, and sustainable dividend payout. *International Journal of Entrepreneurship, 22*(4), 1-9.

Allam, Z., Asad, M., Ali, A., & Ali, N. (2021). Visualization of knowledge aspects on workplace spirituality through bibliometric analysis. *2021 International Conference on Decision Aid Sciences and Application (DASA)* (pp. 446-450). Sakheer: IEEE. doi:10.1109/DASA53625.2021.9682372

Allam, Z., Asad, M., Ali, N., & Malik, A. (2022). Bibliometric analysis of research visualizations of knowledge aspects on burnout among teachers from 2012 to January 2022. *022 International*

Conference on Decision Aid Sciences and Applications (DASA) (pp. 126-131). Chiangrai, Thailand: IEEE. doi:10.1109/DASA54658.2022.9765200

Allen, G. C. (2019). Understanding China's AI strategy: Clues to Chinese strategic thinking on artificial intelligence and national security.

Almansour, A. Z., Asad, M., & Shahzad, I. (2016). Analysis of corporate governance compliance and its impact over return on assets of listed companies in Malaysia. *Science International, 28*(3), 2935-2938.

Almuraqab, N. A. S. (2020). E & M-Government and smart city: A review of ICT strategies and plans in the United Arab Emirates. *International Journal of Management (IJM)*, *11*(3).

Aloul, F. A. (2010, November). Information security awareness in UAE: A survey paper. In *2010 International conference for internet technology and secured transactions* (pp. 1-6). IEEE.

AlQershi, N. (2021). Strategic thinking, strategic planning, strategic innovation and the performance of SMEs: The mediating role of human capital. *Management Science Letters*, *11*(3), 1003-1012.

Alshammari, T. S., & Singh, H. P. (2018). Preparedness of Saudi Arabia to defend against cyber crimes: An assessment with reference to anti-cyber crime law and GCI index. *Archives of Business Research*, *6*(12).

Alshehhi, A. G. (2018). *Strategic Thinking and Strategic Planning: A Conceptual Exposition Through a Case Study of the Police Force in the UAE*. The University of Manchester (United Kingdom).

Al-Suwaidi, J. S. (2018). United Arab Emirates Society in the Twenty-first Century: Issues and Challenges in a Changing World.

Al-Zubaidi, L. S., & Wahab, A. A. A. (2022). The Impact of Knowledge Management on Reducing Digital Crime Levels: Analytical study in the Iraqi Ministry of Interior. *Journal of Positive School Psychology*, *6*(7), 2139-2150.

Amir, A., & Asad, M. (2018). Consumer's Purchase Intentions towards automobiles in Pakistan. *Open Journal of Business and Management, 6*, 202-213. doi:10.4236/ojbm.2018.61014

Asad, M., & Kashif, M. (2021). Unveiling success factors for small and medium enterprises during COVID-19 pandemic. *Arab Journal of Basic and Applied Sciences, 28*(1), 187-194. doi:https://doi.org/10.1080/25765299.2020.1830514

Asad, M., Aledeinat, M., Majali, T., Almajali, D. A., & Shrafat, F. D. (2024). Mediating role of green innovation and moderating role of resource acquisition with firm age between green entrepreneurial orientation and performance of entrepreneurial firms. *Cogent Business & Management, 11*(1), 2291850. doi:https://doi.org/10.1080/23311975.2023.2291850

Asad, M., Asif, M. U., Bakar, L. J., & Altaf, N. (2021). Entrepreneurial orientation, big data analytics, and SMEs performance under the effects of environmental turbulence. *2021*

International Conference on Data Analytics for Business and Industry (ICDABI) (pp. 144-148). Zallaq: IEEE. doi:10.1109/ICDABI53623.2021.9655870

Asad, M., Asif, M. U., Sulaiman, M. A., Satar, M. S., & Alarifi, G. (2023). Open innovation: The missing nexus between entrepreneurial orientation, total quality management, and performance of SMEs. *Journal of Innovation and Entrepreneurship, 12*(79), 1-13. doi:https://doi.org/10.1186/s13731-023-00335-7

Asad, M., Haider, S. H., & Fatima, M. (2018). Corporate social responsibility, business ethics, and labor laws: A qualitative analysis on SMEs in Sialkot. *Journal of Legal, Ethical and Regulatory Issues, 21*(3), 1-7.

Asad, M., Kashif, M., Sheikh, U. A., Asif, M. U., George, S., & Khan, G. u. (2021). Synergetic effect of safety culture and safety climate on safety performance in SMEs: Does transformation leadership have a moderating role. *International Journal of Occupational Safety and Ergonomics*, 1-7. doi:10.1080/10803548.2021.1942657

Asad, M., Majali, T., Aledeinat, M., & Almajali, D. A. (2023). Green entrepreneurial orientation for enhancing SMEs financial and environmental performance: Synergetic moderation of green technology dynamism and knowledge transfer and integration. *Cogent Business & Management, 10*(3), 1-20. doi:https://doi.org/10.1080/23311975.2023.2278842

Asif, M. U., Asad, M., Bhutta, N. A., & Khan, S. N. (2021). Leadership behavior and sustainable leadership among higher education institutions of Pakistan. *Sustainable Leadership and Academic Excellence International Conference (SLAE)* (pp. 1-6). Manama, Bahrain: IEEE Xplore. doi:10.1109/SLAE54202.2021.9788081

Asif, M. U., Asad, M., Kashif, M., & Haq, A. u. (2021). Knowledge exploitation and knowledge exploration for sustainable performance of SMEs. *2021 Third International Sustainability and Resilience Conference: Climate Change* (pp. 29-34). Sakheer: IEEE. doi:10.1109/IEEECONF53624.2021.9668135

Bashir, A., & Asad, M. (2018). Moderating effect of leverage on the relationship between board size, board meetings and performance: A study on textile sector of Pakistan. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS), 39*(1), 19-29.

Bellovin, S. M. (2006). On the brittleness of software and the infeasibility of security metrics. *IEEE Security & Privacy*, *4*(04), 96-96.

Bilal, Z. O., & Sulaiman, M. A. (2021). Factors persuading customers to adopt islamic banks and windows of commercial banks services in Sultanate of Oman. *Review of International Geographical Education(RIGEO), 11*(4), 651-660. doi:10.33403/rigeo. 800679

Blair, J. R., Chewar, C. M., Raj, R. K., & Sobiesk, E. (2020, June). Infusing principles and practices for secure computing throughout an undergraduate computer science curriculum. In *Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education* (pp. 82-88).

Bleijenbergh, R., Mestdagh, E., & Kuipers, Y. J. (2022). Midwifery Practice and Education in Antwerp: Forecasting Its Future With Scenario Planning. *The Journal of Continuing Education in Nursing*, *53*(1), 21-29.

Camtepe, S. A., & Yener, B. (2006). A formal method for attack modeling and detection. *SA Camtepe, B. Yener*.

Chethiyar, S. D., Asad, M., Kamaluddin, M. R., Ali, A., & Sulaiman, M. A. (2019). Impact of information and communication overload syndrome on the performance of students. *Journal of Human and Social Sciences*, 390-406.

Curnin, S., Brooks, B., & Brooks, O. (2022). Assessing the influence of individual creativity, perceptions of group decision-making and structured techniques on the quality of scenario planning. *Futures*, 103057.

Damer, N., Al-Znaimat, A. H., Asad, M., & Almansour, A. Z. (2021). Analysis of motivational factors that influence usage of Computer Assisted Audit Techniques (CAATs) auditors in Jordan. *Academy of Strategic Management Journal, 20*(Special Issue 2), 1-13.

Dixit, S., Singh, S., Dhir, S., & Dhir, S. (2021). Antecedents of strategic thinking and its impact on competitive advantage. *Journal of Indian Business Research*, *13*(4), 437-458.

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*, *8*(1), 1-26.

Fadhel, H. A., Aljalahma, A., Almuhanadi, M., Asad, M., & Sheikh, U. (2022). Management of higher education institutions in the GCC countries during the emergence of COVID-19: A review of opportunities, challenges, and a way forward. *The International Journal of Learning in Higher Education, 29*(1), 83-97. doi:https://doi.org/10.18848/2327-7955/CGP/v29i01/83-97

Farrukh, W., & Asad, M. (2017). The determinants of capital structure: A study on cement sector of Pakistan. *International Journal of Management Sciences and Business Research, 6*(2), 16-26.

Fatima, S. Z., & Asad, M. (2018). Disposal of hospital wastage in Pakistan: A qualitative research. *Advances in Social Sciences Research Journal, 5*(3), 37-42. doi:10.14738/assrj. 53.4197

Flemisch, F., Usai, M., Herzberger, N. D., Baltzer, M. C. A., Hernández, D. L., & Pacaux-Lemoine, M. P. (2022, October). Human-Machine Patterns for System Design, Cooperation and Interaction in Socio-Cyber-Physical Systems: Introduction and General overview. In *2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 1278-1283). IEEE.

Flyverbom, M., & Garsten, C. (2021). Anticipation and organization: Seeing, knowing and governing futures. *Organization Theory*, *2*(3), 26317877211020325.

Furnell, S., Emm, D., & Papadaki, M. (2015). The challenge of measuring cyber-dependent crimes. *Computer Fraud & Security*, *2015*(10), 5-12.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, *35*(2), 486-505.

Haider, S. H., Asad, M., & Almansour, A. Z. (2015). Factors influencing growth of cottage industry in Punjab, Pakistan: Cottage industry owners' perspective. *Paradigms: A Research Journal of Commerce, Economics, and Social Sciences, 9*(1), 78-87. doi:10.24312/paradigms090105

Haider, S. H., Asad, M., & Aziz, A. (2015). A survey on the determinants of entrepreneurial training effectiveness among micro finance institutions of Malaysia. *Mediterranean Journal of Social Sciences, 6*(6 S4), 396-403. doi:10.5901/mjss.2015.v6n6s4p396

Haider, S. H., Asad, M., & Fatima, M. (2017). Responsibility of global corporations towards human resource to attain competitive advantage: A review. *Journal of Research in Administrative Sciences, 6*(2), 9-12.

Haider, S. H., Asad, M., Fatima, M., & Abidin, R. Z. (2017). Microfinance and performance of micro and small enterprises: Does training have an impact. *Journal of Entrepreneurship and Business Innovation, 4*(1), 1-13. doi:https://doi.org/10.5296/jebi.v4i1.10566

Haider, S. H., Fatima, M., Asad, M., & Ahmad, A. Z. (2016). A study on the issues of employment contracts and practices of employment contracts in UAE. *Paradigms: A Journal of Commerce, Economics, and Social Sciences, 10*(1), 58-64. doi: 10.24312/paradigms100105

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. (2010). Multivariate Data Analysis: Pearson Education. Upper Saddle River, New Jersey.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2013). Editorial-partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. *Long Range Planning, 46*(1), 1-12.

Hammami , S. M., Ahmed , F., Johny, J., & Sulaiman, M. A. (2021). Impact of knowledge capabilities on organisational performance in the private sector in Oman: An SEM approach using path analysis. *International Journal of Knowledge Management, 17*(1), 15-18. doi:10.4018/IJKM.2021010102

Hanewald, R. (2008). Confronting the pedagogical challenge of cyber safety. *Australian Journal of Teacher Education (Online)*, *33*(3), 1-16.

Haq, M. A., Asad, M., Natarajan, V., Sankar, J. P., & Asif, M. U. (2021). Microfinance and empowerment: A case study on benificiaries of a community development program. *Turkish Journal of Computer and Mathematics Education, 12*(9), 3282-3288. doi:https://doi.org/10.17762/turcomat.v12i9.5479

Henseler, J., & Fassott, G. (2009). Testing moderating effects in PLS path models: An illustration of available procedures. *Handbook of Partial Least Squares*, 713-735. doi:10.1007/978-3-540-32827-8_31

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115-135. doi:10.1007/s11747-014-0403-8

Hobson, T., Okhravi, H., Bigelow, D., Rudd, R., & Streilein, W. (2014, November). On the challenges of effective movement. In *Proceedings of the First ACM Workshop on Moving Target Defense* (pp. 41-50).

Israr, A., Asad, M., Altaf, N., & Victor, S. (2021). Training effectiveness and performance of micro small and medium sized enterprises. *Turkish Journal of Computer and Mathematics Education, 12*(9), 3289-3295. doi:https://doi.org/10.17762/turcomat.v12i9.5480

Jan, N., Nasir, A., Alhilal, M. S., Khan, S. U., Pamucar, D., & Alothaim, A. (2021). Investigation of cyber-security and cyber-crimes in oil and gas sectors using the innovative structures of complex intuitionistic fuzzy relations. *Entropy*, *23*(09), 1112.

Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., Maddikunta, P. K. R., & Singh, S. (2021). A review on cyber crimes on the Internet of Things. *Deep Learning for Security and Privacy Preservation in IoT*, 83-98.

Karnouskos, S. (2011, July). Cyber-physical systems in the smartgrid. In *2011 9th IEEE international conference on industrial informatics* (pp. 20-23). IEEE.

Kashif, M., Asif, M. U., Ali, A., Asad, M., Chethiyar, S. D., & Vedamanikam, M. (2020). Managing and implementing change successfully with respect to COVID-19: A way forward. *PEOPLE: International Journal of Social Sciences, 6*(2), 609-624. doi:org/10.20319/pijss.2020.62.609624

Khalifa, S. K. H., & Al-Kumaim, N. H. S. (2021). A CONCEPTUAL MODEL FOR PREVENTION OF EFINANCIAL CRIMES IN UAE: A REVIEW PAPER. *Academy of Strategic Management Journal*, *20*, 1-10.

Khalil, R., Asad, M., & Khan, S. N. (2018). Management motives behind the revaluation of fixed assets for sustainability of entrepreneurial companies. *International Journal of Entrepreneurship, 22*(Special), 1-9.

Khan, A. A., Asad, M., Khan, G. u., Asif, M. U., & Aftab, U. (2021). Sequential mediation of innovativeness and competitive advantage between resources for business model innovation and SMEs performance. *2021 International Conference on Decision Aid Sciences and Application (DASA)* (pp. 724-728). Sakheer: IEEE. doi:10.1109/DASA53625.2021.9682269

Khan, M. A., Pradhan, S. K., & Fatima, H. (2017, March). Applying data mining techniques in cyber crimes. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)* (pp. 213-216). IEEE.

Khan, N. S., Chishti, M. A., & Saleem, M. (2019). Identifying various risks in cyber-security and providing a mind-map of network security issues to mitigate cyber-crimes. In *Proceedings of 2nd International Conference on Communication, Computing and Networking* (pp. 93-103). Springer, Singapore.

Khan, S. N., Asad, M., Fatima, A., Anjum, K., & Akhtar, K. (2020). Outsourcing internal audit services; A review. *International Journal of Management, 11*(8), 503-517. doi:International Journal of Management

Khushi, M., din, S. M., & Sulaiman, M. A. (2020). Effects of profitability measures on free cash flow; evidence from pakistan stock exchange . *International Journal of Scientific & Technology Research, 9*(2), 3882-3889.

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*, *2*(1), 191-216.

Majali, T., Alkaraki, M., Asad, M., Aladwan, N., & Aledeinat, M. (2022). Green transformational leadership, green entrepreneurial orientation and performance of SMEs: The mediating role of green product innovation. *Journal of Open Innovation: Technology, Market, and Complexity, 8*(4). doi:https://doi.org/10.3390/joitmc8040191

Makram, H., Sparrow, P., & Greasley, K. (2017). How do strategic actors think about the value of talent management? Moving from talent practice to the practice of talent. *Journal of Organizational Effectiveness: People and Performance*, *4*(4), 259-378.

Malekakhlagh, E., Safari, M., Beigi, S., & Rokhideh, M. R. (2022). Scenario planning and strategic innovation: The mediating effects of strategic thinking and strategic flexibility. *Journal of International Marketing Modeling*, *3*(1), 1-13.

Maness, R. C., & Valeriano, B. (2016). The impact of cyber conflict on international interactions. *Armed Forces & Society*, *42*(2), 301-323.

Miller, B. W., Schuurman, G. W., Symstad, A. J., Runyon, A. N., & Robb, B. C. (2022). Conservation under uncertainty: Innovations in participatory climate change scenario planning from US national parks. *Conservation Science and Practice*, *4*(3), e12633.

Morante, S., Victores, J. G., & Balaguer, C. (2015). Cryptobotics: Why robots need cyber safety. *Frontiers in Robotics and AI*, *2*, 23.

Natcher, D., Owens-Beek, N., Bogdan, A. M., Lu, X., Li, M., Ingram, S., ... & Rice, A. (2022). Scenario planning tools for mitigating industrial impacts on First Nations subsistence economies in British Columbia, Canada. *Sustainability Science*, *17*(2), 469-484.

Nayyar, A. N. A. N. D., Rameshwar, R. U. D. R. A., & Solanki, A. R. U. N. (2020). Internet of Things (IoT) and the digital business environment: a standpoint inclusive cyber space, cyber crimes, and cybersecurity. In *The Evolution of Business in the Cyber Age* (pp. 111-152). Apple Academic Press.

Newton, A. (2014). Ambulance Service 2030: the future of paramedics.

Obeid Alshamsi, A. A., Nusari, M., Abuelhassan, A. E., & Bhumic, A. (2019). Towards a better understanding of relationship between Dubai smart government characteristics and organizational performance. *Development*, *14*(17), 21-23.

Pacaux-Lemoine, M. P., Habib, L., Berdal, Q., & Trentesaux, D. (2021, October). Cooperative patterns or how to support Human-Cyber-Physical Systems cooperation. In *2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 1501-1506). IEEE.

Qalati, S. A., Ostic, D., Sulaiman, M. A., Gopang, A. A., & Khan, A. (2022). Social media and SMEs' performance in developing countries: Effects of technological-organizational-environmental factors on the adoption of social media. *SAGE Open, 12*(2), 1-13. doi:10.1177/21582440221094594

Qalati, S. A., Qureshi, N. A., Ostic, D., & Sulaiman, M. A. (2022). An extension of the theory of planned behavior to understand factors influencing Pakistani households' energy-saving intentions and behavior: a mediated–moderated model. *Energy Efficiency , 15*, 1-21. doi:10.1007/s12053-022-10050-z

Quinlan, C., Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2018). *Business Research Methods* (2 ed.). London: Cengage Learning.

Rajan, A. V., Ravikumar, R., & Al Shaer, M. (2017, June). UAE cybercrime law and cybercrimes—An analysis. In *2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)* (pp. 1-6). IEEE.

Renaud, K., Von Solms, B., & Von Solms, R. (2019). How does intellectual capital align with cyber security?. *Journal of Intellectual Capital*.

Riphah, H. Z., Ali, S., Danish, M., & Sulaiman, M. A. (2022). Factors affecting consumers intentions to purchase dairy products in Pakistan: a cognitive affective-attitude approach. *Journal of International Food & Agribusiness Marketing*. doi:10.1080/08974438.2022.2125919

Salem, S. F., Alanadoly, A. B., & Sulaiman, M. A. (2023). Immersive gaming in the fashion arena: an investigation of brand coolness and its mediating role on brand equity. *Journal of Research in Interactive Marketing*. doi:https://doi.org/10.1108/JRIM-02-2023-0053

Satar, M. S., Alarifi, G., Alkhoraif, A. A., & Asad, M. (2023). Influence of perceptual and demographic factors on the likelihood of becoming social entrepreneurs in Saudi Arabia, Bahrain, and United Arab Emirates – an empirical analysis. *Cogent Business & Management, 10*(3), 1-20. doi:https://doi.org/10.1080/23311975.2023.2253577

Sattar, M. s., Alarifi, G., & Asad, M. (2021). Gaining performance among tobacco sector small and medium enterprises through market orientation. *Tobacco Regulatory Science (TRS), 7*(6-1), 6879-6887.

Shaker, R. Z., Asad, M., & Zulfiqar, N. (2018). Do predictive power of fibonacci retracements help the investor to predict future? A study of Pakistan Stock Exchange. *International Journal of Economics and Financial Research, 4*(6), 159-164.

STEWART, D. H. (2022). INFORMATION TECHNOLOGY AND CYBER SECURITY UNPLUGGED The interrelationship between human, Technology and Cyber Crime Today. *Journal of Digital Information Management*, *20*(2), 75.

Sulaiman, M. A., & Asad, M. (2023). Organizational learning, innovation, organizational structure and performance evidence from Oman. *Organizational Learning, Innovation, Organizational Structure and Performance Evidence from Oman* (pp. 1-17). Ljubljana: The International Society for Professional Innovation Management (ISPIM).

Sulaiman, M. A., Asad, M., Ismail, M. Y., & Shabbir, M. S. (2023). Catalyst role of university green entrepreneurial support promoting green entrepreneurial inclinations among youth: Empirical evidence from Oman. *International Journal of Professional Business Review, 8*(8), e02723-e02723. doi:https://doi.org/10.26668/businessreview/2023.v8i8.2723

Sulaiman, M. A., Asad, M., Shabbir, M. S., & Ismail, M. Y. (2023). Support factors and green entrepreneurial inclinations for sustainable competencies: Empirical evidence from Oman. *International Journal of Professional Business Review, 8*(8), e02724-e02724. doi:https://doi.org/10.26668/businessreview/2023.v8i8.2724

Ta'Amnha, M. A., Magableh, I. K., Asad, M., & Al-Qudah, S. (2023). Open innovation: The missing link between synergetic effect of entrepreneurial orientation and knowledge management over product innovation performance. *Journal of Open Innovation: Technology, Market, and Complexity, 9*(4), 1-9. doi:https://doi.org/10.1016/j.joitmc.2023.100147

Tariq, A., Badir, Y. F., Tariq, W., & Bhutta, U. S. (2017). Drivers and consequences of green product and process innovation: A systematic review, conceptual framework, and future outlook. *Technology in Society, 51*, 8-23. doi:https://doi.org/10.1016/j.techsoc.2017.06.002

Tariq, A., Badir, Y., & Chonglerttham, S. (2019). Green innovation and performance: Moderation analyses from Thailand. *European Journal of Innovation Management, 22*(3), 446-467. doi:https://doi.org/10.1108/EJIM-07-2018-0148

Tariq, A., Ehsan, S., Badir, Y. F., Memon, M. A., & Sumbal, M. S. (2022). Does green process innovation affect a firm's financial risk? The moderating role of slack resources and competitive intensity. *European Journal of Innovation Management*. doi:https://doi.org/10.1108/EJIM-05-2021-0265

Ullah, Z., Otero, S. Á., Sulaiman, M. A., Sial, M. S., Ahmad, N., Scholz, M., & Omhand, K. (2021). Achieving organizational social sustainability through electronic performance appraisal systems: the moderating Influence of transformational leadership. *sustainability, 13*(10), 1-14. doi:0.3390/su13105611

Ullah, Z., Sulaiman, M. A., Ali, S. B., Ahmad, N., Scholz, M., & Han, H. (2021). The effect of work safety on organizational social sustainability Improvement in the healthcare sector: The case of a public sector hospital in Pakistan. *International Journal of Environmental Research and Public Health, 18*(12), 1-18. doi:10.3390/ijerph18126672

Victor, S., ul Haq, M. A., Sankar, J. P., Akram, F., & Asad, M. (2021). Paradigm shift of promotional strategy from celebrity to social CEO. *2021 International Conference on Decision Aid Sciences and Applications (DASA)* (pp. 1016-1023). Zallaq: IEEE. doi:10.1109/DASA53625.2021.9682256

Warner, R. S., & Burton, G. J. S. (2017). The current state of education in the UAE. *Mohammed Bin Rashid School of Government*, *12*(7), 18.

Xie, Z., Qalati, S. A., Sánchez Limón, M. L., Bait Ali Sulaiman, M. A., & Qureshi, N. A. (2023). Understanding factors influencing healthcare workers' intention towards the COVID-19 vaccine. *PLOS ONE, 18(7)*, e0286794. doi:doi.org/10.1371/journal.pone.0286794

Yaser Alraei, A. B. A., Joseph, A., Asif, M. K., & Hock, O. Y. (2020). Application of Strategic Management Information System (SMIS) in the Ministry of Interior, UAE: Issues and Challenges. *International Journal of Academic Research in Business and Social Science*, *10*(2), 346-361.

Younies, H., & Na, T. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*, *27*(4), 1089-1105.

Zahed, B. T., White, G., & Quarles, J. (2019, September). Play it safe: An educational cyber safety game for children in elementary school. In *2019 11th International Conference on Virtual Worlds and Games for Serious Applications (VS-Games)* (pp. 1-4). IEEE.

Zahid, H., Ali, S., Danish, M., & Sulaiman, M. A. (2022). Factors affecting consumers intentions to purchase dairy products in Pakistan: A cognitive affective-attitude approach. *Journal of International Food & Agribusiness Marketing, 1-26*. doi:https://doi.org/10.1080/08974438.2022.2125919

Zahra, K., Majeed, K., Mahmood, A., & Asad, M. (2012). Impact assessment of community participation in solid waste management projects in selected areas of Faisalabad city. *Journal of Urban Planning and Development, 138*(4), 319-327. doi:10.1061/(ASCE)UP.1943-5444.0000127

Zuhaib , Z., Wenyuan, L., Sulaiman, M. A., Siddiqu, K. A., & Qalati, S. A. (2022). Social entrepreneurship orientation and enterprise fortune: an Intermediary role of social performance. *Frontiers in Psychology, 12*, 1-17. doi:10.3389/fpsyg.2021.755080