Indian Journal of Economics and Business
Vol. 20 No. 4 (July-December, 2021)

http://www.ashwinanokha.com/IJEB.php

Review of Scoping Studies on Improving Physical Security Performance and Integrating Facial Recognition Technology

Saeed Al Zaabi [1], **Ruzaidi Zamri** [2]

[1] *Technology Management and Entrepreneurship Faculty, Universiti Teknikal Malaysia Melaka, Malaysia*, sss2111567@gmail.com

[2] *Manufacturing System Engineering Faculty, Universiti Teknikal Malaysia Melaka, Malaysia*, ruzaidi@utem.edu.my

Corresponding Author: sss2111567@gmail.com

Received: 06th October 2021
Revised: 19th November 2021
Accepted: 06th December 2021

Abstract: High risk sectors such as oil and gas sectors, provision of security is usually not negotiable. Formidable infrastructure is normally required to achieve protection and sustainability. Many companies in the oil and gas industry have invested hugely in security to ensure continuity of operations thus amassing considerable profits. The advancement in technology has seen the industry advance in its security by incorporating a variety of technologies centered on advancing security. One such technology has been the facial recognition technology (FRT). As such, the main objective of this review article is to focus on analyzing the available literature on integrating FRT with the physical security cultures of organizational, human, and technological domains in gas and oil companies and how it can improve physical security performance. The review focused on empirical studies on effectiveness of subdomains elements in the development of positive physical security culture. Further, it explored the efficacy of FRT in enhancing the efficiency of physical security systems. The review thus did conclude that, there was a clear link between the physical security culture domains and the physical security performance. Therefore, the main narrative of the review was the need to improve the physical security performance through the integration of FRT into their overall security framework. Through the analysis of the available literature, the study revealed there is a platform to improve the physical security performance by utilizing the affordances of FRT and an integrated physical security system. The reviewed empirical studies also led to the development of new conceptual framework for research aimed at investigating how best FRT can be integrated effectively in physical security. This study may add to the understanding of the circumstances under which companies consider their physical security to vulnerability and thus need improvement.

Keywords: physical security threats; facial recognition technology; physical security gaps; physical security culture; physical security domain.

1. Introduction

Feeling safe is something that many individuals don't for granted since the world is camouflaged with all manner of insecurity. Besides the need to protect ourselves, protection of assets is also fundamental. Over the years, the need to protect assets of organizations or companies from unauthorized personnel has transformed into topical issue. Companies have incorporated different means to effectively protect their assets from being accessed by unauthorized people. Technology related security has gained a lot of prominence in the recent past thanks to its effectiveness. Nonetheless, several studies done have still reported that organizations are still exposed to threats such as vandalism, theft or sabotage. This has been based on the fact that as technology continues to grow, perpetrators also devise various ways of actualizing their acts. As such, this has presented novel and sophisticated challenges for physical security teams. Leading companies in the gas and oil sector have not been spared in these breaches. For instance, Saudi Aramco, one of the world's largest companies in the oil and gas industry, faced several security incidents recently despite investing in the security of its networks and deploying 33,000 soldiers and 5,000 guards to protect the company's assets (Alelyani and Kumar, 2018). These happenings have created a lot of tension in the industry thus triggering the need for scholars to conduct research on ways the existing physical security systems can be strengthened and also develop new strategies that aim at providing effective and efficient solutions.

Physical security has over the recent years been a gradually developing matter and it currently plays a central role in energy production for the region. Various physical security control systems, such as CCTV surveillance, security officers, protective barriers, locks, accesscontrol, perimeter intrusion detection, and fire protection, are currently being utilized to restrict access to certain areas in this sector (Walton, 2016). Regardless, sufficient evidence suggests that many organizations continue to struggle with complex security threats because their systems do not address inherent vulnerabilities (Swanson, 2020). Ruwais Refinery is an example of critical oil and gas facilities in the Emirate where some organizations remain exposed to physical security risks. According to Barnes et al. (2019), industries have had to adopt a systematic and strategy-linked approaches to provide an efficient framework for improving physical security performance.

The goal of improving physical security is frequently disregarded. Its significance is often underrated in favor of more technical threats, such as hacking, terrorism, crypto viral exertion, and cyber espionage (Awasthi and Grzybowska, 2019). Such inclinations have resulted in severe physical security breaches leading to huge losses (Walton, 2016). By not enforcing the company policies and security procedures, security control personnel have multiplied the physical security systems gaps (Swanson, 2020). This fact has led to more recent studies focusing on identifying possible vulnerabilities of the current security measures, discovering and investigating potential improvements to address the gaps. Therefore, one of the dominant issues is that organizations adopt new technologies without meeting the prerequisites that promote efficiency.

The available evidence provides a compelling reason to believe that integrating facial recognition technology with the existing physical security systems in companies could improve the effectiveness of technological, organizational, and human domains of physical security culture (Yasseri, 2019). Unfortunately, the existing literature does not provide important data on the applicability of facial

recognition technology for enhancing the elements of subdomains across the domains of physical security culture. Therefore, this review may be considered as one of the first attempts to investigate the integration of facial recognition technology into the existing security domains to enhance the physical security systems. The review is expected to address an evident research gap and, at the same time, produce valuable findings that could be used for developing and provide recommendations to enhance the physical security system

2. Scoping Review and Research

Scoping studies represent an increasingly popular approach to reviewing research evidence. However, no universal scoping study definition or purpose exists. Definitions commonly refer to 'mapping,' a process of summarizing a range of evidence in order to convey the breadth and depth of a field. Scoping studies differ from systematic reviews because authors do not typically assess the quality of included studies. Scoping studies also differ from narrative or literature reviews in that the scoping process requires analytical reinterpretation of the literature (Yas, Jusoh, Abbas, Mardani, & Nor, 2020). Researchers can undertake a scoping study to examine the extent, range, and nature of research activity, determine the value of undertaking a full systematic review, summarize and disseminate research findings, or identify gaps in the existing literature. As such, researchers can use scoping studies to clarify a complex concept and refine subsequent research inquiries. Scoping studies may be particularly relevant to disciplines with emerging evidence, such as rehabilitation science, in which the paucity of randomized controlled trials makes it difficult for researchers to undertake systematic reviews (Khudhair, Jusoh, Mardani, Nor, & Streimikiene, 2019). In these situations, scoping studies are ideal because researchers can incorporate a range of study designs in both published and grey literature, address questions beyond those related to intervention effectiveness, and generate findings that can complement the findings.

The field of physical security is also actively incorporating scoping review due to the ever changing world of technology that is transforming the sector rapidly. Besides, theoretically, the findings of the research and the reviews are used to map all fields of studies because it is difficult to imagine the scope of material used and the evidences being accessible. This review purposed to examine how physical security performance could be improved through integration of facial recognition technology. The underlying aim was anchored on recognizing the difficulties encountered when obtaining evidence of findings in areas where no research has been conducted thus distinguishing the significance of methodical studies in areas of research endeavor. As such, this aspect seeks to show that distinguishing gaps in literature through a scoping study won't really recognize the research gaps where research itself is of low quality since it does not shape some portion of the study.

In many sectors, the thought of security assumes the fundamental role in affecting the satisfaction of companies. These is based on the fact that different companies in the sector use different forms of physical security and to some extent, they find them satisfactory Inasmuch as that is the case, Hutter (2016) points out that the prioritization of physical security in the overall information security system is usually low. In most situations, stakeholders focus on technology-based security breaches rather than physical threat exposure (Kashwani, 2017). As a result, many organizations have low resilience toward physical security threats. Many studies explore the significance of physical security gaps that emerged due to the ineffectiveness of specific elements, such as CCTV surveillance systems or security officer patrols (Yang

et al., 2019). It was found that facial recognition technology could help address most of these vulnerabilities (Al-Khouri, 2012). Simultaneously, it remains unclear how and to what extent the integration of this technology could improve the technological, organizational, and human domains of the physical security culture of critical oil and gas facilities in Abu Dhabi, which constitutes an evident research gap. Also, measurement of physical security performance remains a controversial and challenging issue. In order to assess a firm's resilience towards physical security threats, scholars would need to have access to detailed information about an organization's physical security measures and their vulnerabilities, which is hardly possible in most situations.

The concept of a physical security culture is directly connected with organizations' resilience towards physical security threats. Unfortunately, the task of creating and maintaining such a culture remains evasive due to challenges accompanying the process of combining measures associated with three domains of a physical security culture. According to Landucci et al. (2020), all the elements of the subdomain should be measured to address the physical security culture of an organization. The effectiveness of these elements in the subdomain affect the domains of the physical security culture which determines the performance of the physical security in an organization. The idea of emphasizing security culture when discussing security threats is barely novel. The literature indicates that understanding a security culture as a set of values, principles, policies, and assets predetermining a firm's resilience towards security threats has been among the most popular approaches towards conceptualizing organizational security for decades (Swanson, 2020). Nonetheless, recent developments have led to the reinterpretation and re-conceptualization of the notion of a security culture due to the growing realization of the fact that organizational security cannot be ensured unless all the security components are linked together with the help of an influential security culture (Sas et al., 2020). Therefore, using a conceptual framework on physical security culture to discuss and analyze the physical security performance of companies seem to be a rational option aligned with recent security studies' trends.

3. Methodology

The scoping review method that was originally advanced in Arksey and O'Malley and later improved and elaborated in Levac and recommended in Colquhoun was adapted in the scoping review (Yas, Alkaabi, Al Mansoori, Masoud, & Alessa, 2021). The procedure for scoping review methodology involved five-step heuristic that include identifying research question, identifying relevant studies, study selection, charting the data, and collating, summarizing results and reporting the results.

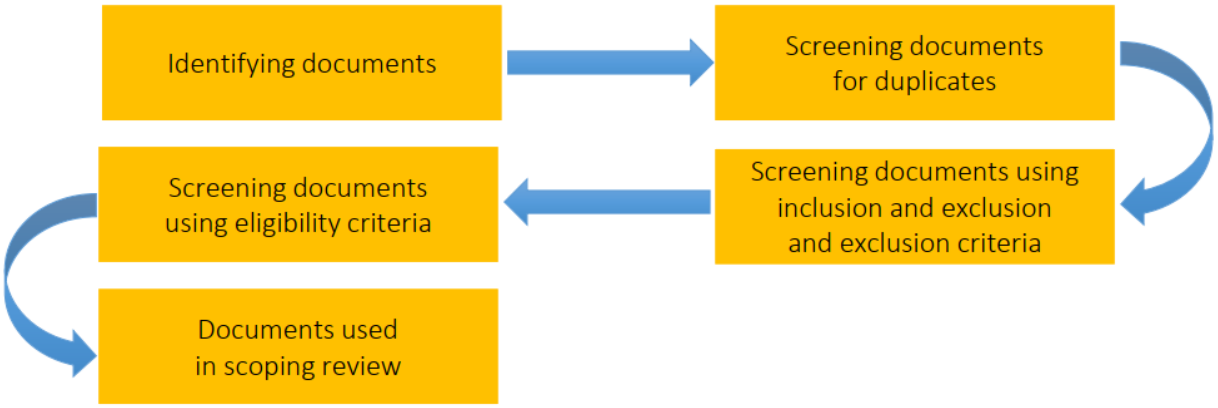

Figure 1: Scoping Review Process

3.1 Identifying Research Questions

The commencement stage for scoping review is usually the identification of research question just like in literature reviews. As such, the research questions were identified and this step was helpful with regard to choosing the appropriate methodology to use. Consideration on appropriate features of the research question is usually essential for instance, the research populace, intercessions or results. It is suggested that the integration of facial technology will go a long in improving the performance of physical security. This thought is based on the fact that since several companies are already using other forms of technology enabled physical security and still there is an issue security threat, then the facial recognition may help solve the problem.

Across the world, UAE has been regarded as a pioneer in biometric implementation. It has integrated multiple biometric technologies in critical infrastructure systems in the last decade to enhance security and protect its citizens and the nation. Biometrics features, such as facial recognition technology, are already being used at airports and the police force, which has helped the UAE government combat crime and reduces potential security risks in the country. A facial recognition system is being tested in the UAE to enable a moving police patrol car to recognize the presence of a wanted person in public (George, 2015). Various technologies are used at airports to screen passengers passing through immigration controls, such as ocular-based scanning and facial recognition. The integration of facial recognition technologies with video surveillance systems allowed Dubai police to arrest 319 suspects in 2019 (Al Shouk, 2019). Therefore, the notion of facial recognition and other biometric features is hardly novel for the Emirate and the country.

On the other hand, many oil and gas facilities in Abu Dhabi have not implemented facial recognition technology in the physical security systems. Going through the entire Abu Dhabi Safety and Security Planning Manual, it becomes evident that facial recognition technology is not mentioned as a relevant physical security aspect. However, surveillance and other protection forms have been detailed (Abu Dhabi Urban Planning Council, 2014). The manual provides some information regarding the protection of

industrial property, staff, and visitors. It recommends supporting the use of active systems that should be developed following a safety and security risk assessment (Abu Dhabi Urban Planning Council, 2014). Simultaneously, the document lacks information on the technological viewpoint of security implementation in the oil and gas industry, multiplying the challenges of securing oil and gas companies' assets from internal and external threats. Therefore, this does point out that it is key that another technology such as the facial recognition technology developed and implemented to save assets.

3.2 Identifying Relevant Studies

A strength of scoping studies includes the breadth and depth, or comprehensiveness, of evidence covered in a given field. However, practical issues related to time, funding, and access to resources often require researchers to consider the balance between feasibility, breadth, and comprehensiveness. Brien *et al.* reported that their search strategy yielded a vast amount of literature, making it difficult to determine how in depth to carry out the information synthesis. Although Arksey and O'Malley identify these concerns and provide some suggestions to support these decisions, we also struggled with the trade-off between breadth and comprehensiveness and feasibility in our scoping studies (Arksey and O'Malley, 2005). As such, it is recommended that researchers ensure decisions surrounding feasibility do not compromise their ability to answer the research question or achieve the study purpose. Second, it is recommended that a scoping study team be assembled whose members provide the methodological and context expertise needed for decisions regarding breadth and comprehensiveness. When limiting scope is unavoidable, researchers should justify their decisions and acknowledge the potential limitations of their study. In this study, reviewing time, language, and range limitations, studies from 2005 to 2021 are included. The start date was picked to acknowledge significant changes and also given the fact that career assistance is somewhat a recent tool. Companies face different physical security threats related to weaknesses in their physical security cultures' technological, organizational, and human domains (Yasseri, 2019). When these companies are clustered together, a physical security threat affecting one of these companies affects other firms in the area in one way or another. To understand the effects, it is critical to assess the domains of the physical security culture which determines the performance of the physical security in an organization.

The organizational domain of physical security culture consists of tangible aspects of security in an organization such as company policies and security procedures. Company policies are essential components of the organizational environment. These refer to general guidelines with which all the employees are supposed to comply to prevent the firm's assets from internal and external physical security threats. An analysis of the academic literature illustrates that employees' awareness of company policies positively affects organizational security (Campbell, 2014). The realization of company policies is supposed to be an overarching principle integrated into each staff member (Alqahtani, 2017). Therefore, it seemed appropriate to consider company policies as an essential independent variable in this research.

Security procedures are closely connected with the company policies. Simultaneously, their impact on physical security is even more explicit than in the case of company policies (Harris, 2013). Stewart et al. (2012) argue that physical security procedures constitute a crucial aspect of physical security requirements. Unfortunately, most studies dedicated to organizational security procedures focus on information security rather than physical security (R. Ali et al., 2020). At the same time, it is important to emphasize that while

scholars distinguish between physical security and other forms of security, most scientists recommend implementing security procedures as a holistic system that includes physical, information, and other procedures (Sinha et al., 2015). Nonetheless, it could be inferred from the literature that adherence to organizational security policies is supposed to be a crucial driver of physical security in any industry (Fennelly, 2017). The importance of organizational security procedures is the main reason behind the author's decision to use them as one of the study's independent variables.

The technological domain of physical security culture consists of security technology, material, and equipment in an organization. Traditional physical security controls, such as locks and keys, doors, gates, and barriers,are physical security measures widely used to protect the assets and employees throughout the industry to deter and detect physical security threats such as penetrators from entering critical facilities. Nevertheless, these physical security measures' limitations and vulnerabilities can beeasily exploited by determined criminals because of flaws in a physical security system's organizational or human domains (Hassaballah and Aly, 2015). The academic literature illustrates that locks, keys, doors, gates, and barriers alone are insufficient to provide an adequate security level. The effectiveness of these traditional security measures depends on security officers' ability to monitor the traffic in and out of restricted facilities by controlling each individual's authorization level.

Organizations in the oil and gas industry have tried therefore tried to apply technologies that could deter crimes highlighted above. To address the problem that rush hours are seen as an opportunity to commit illicit activities and chances of admitting unauthorized individuals into the facility, modern forms of technological systems, such as fingerprint technology, CCTV cameras and electronic control systems have been used but unfortunately criminals have become more sophisticated thus undermining the effectiveness of these systems. For with fingerprints, these criminals have been known to use compromised templates to clone fingerprints and access restricted facilities (Schwarzl and Weippl, 2011). Naturally, such actions pose a significant threat to individuals, companies, and the entire industry. For CCTV surveillance system's efficiency depends on the security officers monitoring the screen's activities; accordingly, it touches the technological domain, the organizational and human domains of a physical security culture. If security officers are not alert to respond to any suspicious event, they will fail to detect and react to any breaches. Naturally, security officers cannot look at CCTV monitor screens for hours without getting exhausted, magnifying the riskof overlooking criminal acts or other events threatening an organization's security (Fennelly, 2017). Several methods have been introduced to address this problem, including changing the shifts of security officers monitoring the CCTV at intervals, having fewer monitor screens, andarranging the monitors in such a way that does not cause fatigue (Fennelly, 2017). All these methods have the potential to increase the organizations' resilience towards physical security threats.

Concerning human domain of physical security culture, it consists of less tangible or non-observable security aspects in an organization. An example of non-observable security elements in an organization could be the physical security's effectiveness as perceived by the employees. Security officers represent an organization's image and play a crucial role in protectingany entity's assets, information, and employees. Ensuring that all areas within the company areprotected is a challenging process. Therefore, it is evident that there needs to be an action that requires execution to ensure the effectiveness of physical security system. The facial recognition technology offers a good avenue to satisfy this need thereby ensuring assets are secure. Already the country is known to be the pioneer of biometric technology. The technology has been included in key infrastructural systems to enhance security and protect citizens and the nation. Several sectors have been lagging behind in upgrading their security systems to coincide with new developments in the security world. It is key that the sector develops an integrated physical security framework that will be key in introducing facial recognition technology.

3.3 Study Selection

The study's scoping search was carried in academic databases that included academic Search premier; Industry Source Premier; Emerald Full content and Emerald understanding; Taylor and Francis; Sage Publication; EBSCO; Web of Knowledge and Google Scholar; ProQuest (USA Thesis); Directory of Open Access Journals (DOAJ); As can be found in the literature review, particular articles were checked from 2005 to 2021.

3.4 Charting the Data

This stage involved the extraction of data from included studies. To clarify this stage, it is always recommending that the research team collectively develop the data-charting form to determine which variables to extract that will help to answer the research question. Also, it is recommending that charting be considered an iterative process in which researchers continually update the data-charting form. The diagraming approach which is similar to account view was used.

Author(s) of research paper	Title of research and Year of publish	Objectives of the research	Methodology used	Parameters, Methods, Tools	Strengths and weakness	Research gaps in the paper
Albattat & Mat Som	Biometric Technologies in Emergency Management: The Case of Hotels (2014)	To design a model for the effective evaluation of a physical protection system	The authors do not use empirical data. The researchers utilized cloud generation algorithms to construct a model on the basis of the literature review's findings	The model for evaluating physical protection systems' effectiveness. Specific tools incorporated into the model includes face recognition, fingerprint, hand geometry, and iris technologies.	The authors managed to create a new model for evaluating the effectiveness of a physical protection system. The model's novelty and its basis of credible quantitative data are the key strengths of the study. A failure to explain the model's integration with other security pillars and questionable external validity are the study's weaknesses.	The integration of physical security with other domains of security, the relationship between objective and subjective factors in the evaluation of physical security risks
Lichte & Wolf	A study on the influence of uncertainties in physical security risk analysis (2018)	To evaluate the impact of uncertainties on the analysis of physical security risks	The quantitative methodology used in this study is based on the use of experts' knowledge for conducting a quantitative risk assessment	The proposed model operates with such parameters as attacks, threats, consequences, and rankings. Countermeasures are analyzed based on protection, observation, and intervention characteristics	Strengths: the incorporation of uncertainties into the assessment of physical security risks, a high level of validity due to the use of experts' knowledge. Weaknesses: input parameters for consequences and threats are not sufficiently detailed, the lack of attention to the integration of physical and other security risks	The paper does not consider both objective and subjective factors in analyzing the impact of different security risks on the vulnerability assessment
Titu, Pop, & Ceocea	Risk assessment on physical security within a technologized knowledge based organization (2019)	To explore the decision making process involved in risk management on the basis of the established hierarchy of risks	Grounded theory	Physical security risks and response strategies	Strengths: a link between physical security risks and response strategies, the investigation of various relevant risk-based events, a detailed analysis of a risk profile. Weaknesses:	The paper does not analyze universal risk scenarios and physical risk assessment, as the study's focus is put on a technologized knowledge-based organization
Timbs	Physical security assessment of a regional university computer network (2013)	To conduct a detailed evaluation of physical security risks facing a university's computer network	The author relied on secondary data and the research philosophy of pragmatism to construct an effective physical security assessment tool	PSATool operating with a limited set of physical security risks	Strengths: an identification of a significant number of risks, the presentation of the tool's usability and wide applicability, a successful confirmation of the tool's effectiveness based on a particular case study. Weaknesses: a limited scope of the tool, its primary focus on a university-based computer network	It is not clear how the tool could be used to analyze non-physical security risks, as the interaction of different groups of risks is not covered in the study

Review of Scoping Studies on Improving Physical Security Performance and Integrating Facial Recognition Technology

Author(s) of research paper	Title of research and Year of publish	Objectives of the research	Methodology used	Parameters, Methods, Tools	Strengths and weakness	Research gaps in the paper
Ali & Awad	Cyber and physical security vulnerability assessment for IoT-based smart homes (2018)	To carry out the quantitative assessment of physical security risks at smart homes	The operationally crucial threat, asset, and vulnerability evaluation methodology	OCTAVE Allegro focusing on 40 security risks facing smart homes	Strengths: the identification of specific physical and cyber threats facing smart homes, the description of threats' potential consequences, the focus of both cyber and physical security threats at the same time, the development of promising countermeasures against threats. Weaknesses: a limited scope of the study that does not go beyond security threats facing smart homes	The study has a limited external validity; therefore, its findings cannot be used for analyzing physical security threats of any other organizations besides smart homes
Drago	Methods and techniques for enhancing physical security of critical infrastructures (2015)	To design instruments for improving integrative security systems to ensure a sufficient protection level	A mixed methodology and a two-phase approach using the vulnerability assessment and the interoperability framework	The proposed model includes 27 parameters, such as the number of attackers, the number of security officers, a fence's failure rate, and others.	Strengths: an integrative approach towards evaluating and improving physical security, the use of a series of measures to ensure a multilevel protection system, facial recognition technology is integrated with other security technologies Weaknesses: the research is primarily based on the railway industry	The study's findings apply primarily to the railway sector and mainly focus on technological aspects of physical security
Virtanen	The security model to combine the corporate and information security (2001)	To create a model combining corporate and information security layers	The study is based on secondary data	9 domains of corporate security, including physical, personal, information, administrative, and technological security as well as fire prevention, emergency supply, safety, and environmental protection.	Strengths: the proposed model incorporates both information and corporate security levels Weaknesses: the study might be considered obsolete, the issue of corporate security is not sufficiently addressed.	The research does not address modern technologies, such as facial recognition technologies
Graves	Analytical foundations of physical security system assessment (2006)	To design an analytical framework for measuring physical security risks	Linear programming	The dual problem aimed at identifying a security system's vulnerabilities	Strengths: the model addresses various physical security risks and applies it to a specific scenario. Weaknesses: the study is limited to a military scenario	The study's findings have limited external validity due to the focus on the military base and, therefore, could be hardly applied for a non-military organization
DeSmit, Elhabashy, Wells, & Camelio	Cyber-physical vulnerability assessment in manufacturing systems (2016)	To create a model for evaluating cyber-physical vulnerabilities of manufacturing systems	Intersection mapping and the vulnerability impact analysis	Low, medium, and high vulnerabilities	Strengths: the development of a model distinguishing between three levels of cyber-physical vulnerabilities, a relatively high level of flexibility. Weaknesses: a failure to explain the interaction between cyber and physical security risks, insufficient attention to counter measures	The research primarily focuses on vulnerabilities and of manufacturing systems; thus, its contributions to the existing knowledge of physical security evaluation are limited
Alach	Mapping the elements of physical security towards the creation of a holistic physical security model (2007)	To generate new knowledge concerning physical security risks	The quantitative methodology and the research method of a survey	Mathematic tangent functions measuring physical security arrangements	Strengths: the study's conceptual mapping claims to be universal, proposed scenarios cover the majority of physical security threats. Weaknesses: the knowledge generated in the study seems generic.	The relationship between different layers of security is not addressed in detail.

Author(s) of research paper	Title of research and Year of publish	Objectives of the research	Methodology used	Parameters, Methods, Tools	Strengths and weakness	Research gaps in the paper
Wu, Kang, & Li	Risk assessment method for cyber security of cyber physical systems (2015)	To design a model for evaluating cyber security risks of cyber physical systems	The study is based exclusively on secondary data	The risk assessment algorithm specifying responses to various attacks on a cyber-physical security system	Strengths: the proposed model offers a new algorithm for addressing attacks both at the system and the host levels. Weaknesses: the model includes only four types of criteria.	The model mainly focuses on cyber threats; thus, its value for the assessment of physical risks is limited.
Shohaieb, Hashem, & Hanafy	Effect of physical security initiatives on supply chain performance (2018)	To explore the influence of physical security measures on the performance of supply chains	A mixed research methodology (semi-structured interviews and a survey)	Physical security and supply chain performance (agility, responsiveness, cost, reliability, and suppliers' performance)	Strengths: the identification of specific benefits of improved physical security systems for supply chains and the presentation of valuable insights for integrating physical and logical security layers. Weaknesses: the physical security layer is not scrutinized in the study; furthermore, there is no distinction between different elements of the technological, human, and organizational layers.	The study's findings are generic and mainly focus on supply chain management; thus, its insights for the evaluation of physical security risks and measures are constrained.
Horne, Ahmad, & Maynard	Information security strategy in organizations: Review, discussion and future research directions (2015)	To provide relevant recommendations for organizations concerning the creation of a holistic security model to protect their assets	A thematic review of the literature	Individual, group, organization, and inter-organizational layers of security integrated into a model with antecedents, ISSiO constituents, and yields.	Strengths: a clear definition of an information security strategy and a strategic view of security in the organizational environment. Weaknesses: specific measures of an information security strategy are not sufficiently discussed.	The study's findings cover physical security only partially. Furthermore, the research does not address the interaction between different measures of a security system and organizational policies and employees' behavior
Yaccoub et al.	Cyber-physical systems security: Limitations, issues and future trends (2020)	To identify and describe the key facets of cyber-physical systems	Systematic literature review	CSR security vulnerabilities, attacks, and threats as well as corresponding applications and technologies	Strengths: the use of recent data, an attempt to link security vulnerabilities and gaps to security risks, an emphasis on the integration between cyber and physical security layers. Weaknesses: the scope of physical security threats and risks reviewed in the study is slight.	Research gap: the study does not show the interaction between organizational, human, and technological layers of security, as the primary focus is put on technological aspects.
Hassan, Ismail, & Maarop	Information security culture: A systematic literature review (2015)	To determine and discuss factors affecting an information security culture	Systematic literature review	Security behavior, security awareness, top management, cultural differences, trust, information sharing, security policy, security knowledge, belief	Strengths: the use of recent data, the incorporation of findings from various studies, the discussion of some under-researched areas of security, such as employees' security behavior. Weaknesses: the authors' failure to incorporate their findings into a universal security model, the lack of clarity in regard to certain factors influencing security, factors' overlapping.	The study does not cover technological aspects of security and does not provide sufficient details about the interaction between various factors identified in the research. Furthermore, the results of this research mainly apply to the healthcare sector.

The table above shows that contemporary literature offers limited insights into physicalsecurity in the organizational environment. Many studies provide limited findings that only apply to specific industries or cases, while others fail to explain the interaction between physicalsecurity measures and

other types of security controls. Furthermore, most research does not explain how technological, organizational, and human domains of a physical security culture interact with each other, which results in the vague understanding of a physical security system. It is also important to emphasize that the lack of sufficient details about specific physical security controls makes it hard to project the performance of new security controls, such as facial recognition technology. Suppose this technology is integrated into the existing physical security system. In this situation, it seems justified to conclude that the chosen research problemand the study's scope are promising.

3.5 Collating and Reporting

This stage of the study that is concerned with the gathering or evaluation of information for the literature review is very critical. The review involves perusing, examining, reviewing and evaluating an extensive corpus of studies even though it is only a small portion of the analysis that can be incorporated into the final report. The section usually endeavors to show diagram of all the evaluated materials and the presentation of the conceivably substantial assemblage of the materials. Scoping study requires logical system or topical development to exhibit evidence of the current accessible literature, and no attempt is made to introduce the reviews with regard to the value of the findings and evidence in relation to specific mediations or strategies while trying to understand the meaning the scoping study and the broader implications for research, policy and practice. As such, this leads to the final stage of the framework.

3.7 Consultation

The consultation stage is usually an optional stage though it is being argued that it contributes to the methodological rigor and thus it needs to be considered as a required component. In this study, the experiences gained were helpful in the methodological stage. The analysis of the articles revealed that facial recognition applications could reduce the impact of internal and external physical security threats. In particular, the technology could provide organizations with an opportunity to automatically grant or deny access by verifying the authorization through the comparison of the individuals' identity with the recordsof enrolled employees in the database, as opposed to manually verifying their identities with the help of ID cards (Hassaballah and Aly, 2015). Simultaneously, there are specific challenges to implementing the technology, especially those connected with the organization's logistical aspects and maintaining effective physical security measures. The arguments above illustrate that while the technology could reinforce the physical security system's technological domain, its implementation might be accompanied by significant challenges in logistical aspects. Still, its implementation could provide substantial relief, as it has proven to be effective in enhancing the levels of security in many sectors, including air travel, banking, and public administration (Al Ramahi, 2018). In this situation, it seems justified to shift the discussion's focus to particular areas in which technology implementation could be exclusivelyeffective.

One of the most evident facial recognition technology applications is the prevention of unauthorized access to restricted facilities. This aspect of the existing security systems is challenging because organizations should ensure the continuous operation of the existing security measures to

assess whether facial recognition instruments have improved their physicalsecurity performance (Rouse, 2016). At this stage, the technology could be primarily used as avaluable addition to electronic access cards. In theory, a system relying on such cards is sufficient, but if a card is stolen, an unauthorized person could use it to gain access to restrictedareas (Hutter, 2016). An organization that has successfully integrated facial recognition technology into its physical security system would effectively prevent this risk because an unauthorized person would inevitably fail the verification process.

Another promising area of the technology's implementation is processing high personnel volumes during rush hours. As stated above, the risks of providing unauthorized individuals with a right to access restricted facilities magnify during rush hours because security officers might not have enough time to examine the situation (Swanson, 2020). Integrating facial recognition technology into the existing security measures to interrupt people's flow from one area to another could reduce the chances of admitting unauthorized individuals. NEC Corporation (2017) has developed a video face recognition application that could identify individuals accurately and effectively even if they move in large groups. Personnel might not even be aware that the process takes place as they arrive or leave their workplace. This same application could also automatically increase perimeter surveillance's effectiveness, possibly alerting the physical security team of unauthorized individuals gaining access to restricted areas.

If placed correctly during an incident and emergency evacuation, facial recognition technology can identify individuals gathering at the emergency assembly point. A surveillance system integrated with facial recognition technology could quickly locate missing persons at the emergency assembly point (Albattat and Mat Som, 2014). Real-time tracking of these missingpersons exact locations could be pinpointed, which would allow the Incident Management Team to dispatch response teams within a short time to save their lives (Hutter, 2016). This technology will have a more effective emergency response approach than monitoring CCTV cameras or punching system logs to trace the last position where a missing person had been. UAE is among the many countries where facial recognition technology is becoming increasingly popular. At the beginning of 2021, the Cabinet, led by Sheikh Mohammed, approved facial recognitiontechnology implementation "in some private-sector services to verify individuals' identities instead of submitting many documents" (Nasrallah, 2021). Government officials expect facial recognition technology powered by artificial intelligence will significantly increase many private organizations' physical security levels (Hilotin and Pulikkal, 2021). In light of these developments, it seems justified to expect that facial recognition technology will continue expanding its presence in the UAE.

4. Finding & Discussion

The research evidence and experience gained from this study points out that there is no definite procedure that has proven effective when scoping for literature review. Thus, the framework incorporated is not presented as the only methodological approach. The findings revealed that there is a strong positive link between the integration of facial recognition technology and physical security culture. Even though it may not be a hundred percent effective, it is better compared to other forms of technologies used in security.

Conclusion

Companies usually face different physical security threats related to weaknesses in their physical security cultures' technological, organizational, and human domains. When these companies are clustered together, a physical security threat affecting one of these companies affects other firms in the area in one way or another. This research examined the integration of facial recognition technology with existing physical security culture's domains used to improve the physical security performance. It investigated how the integration of facial recognition technology could improve the firm's physical security performance within the physical securityculture's organizational, technological, and human domains.

Acknowledgment

We thank Universiti Teknikal Malaysia Melaka (UTeM) for facilitating this study and for continuous support.

REFERENCES

Abu Dhabi Urban Planning Council. (2014). Abu Dhabi Safety and Security Planning Manual. Abu Dhabi Urban Planning Council. https://jawdah.qcc.abudhabi.ae/en/Registration/QCCServices/Services/STD/ISGL/ISGL-LIST/DP-305.pdf

Al Ramahi, N. (2018). Cameras with facial recognition software will identify wrongdoers in Dubai. The National. https://www.thenationalnews.com/uae/cameras-with-facial-recognition-software-will-identify-wrongdoers-in-dubai-1.699321

Al Shouk, A. (2019). How Dubai's AI cameras helped arrest 319 suspects last year. Gulf News. https://gulfnews.com/uae/how-dubais-ai-cameras-helped-arrest-319-suspects-last-year-1.62750675

Albattat, A., and Mat Som, A. P. (2014). Biometric Technologies in Emergency Management: The Case of Hotels. International Journal of Tourism & Hospitality Reviews, 1, 44–50. https://doi.org/10.18510/ijthr.2014.115

Alelyani, S., and Kumar G R, H. (2018). Overview of Cyberattack on Saudi Organizations.

Al-Khouri, A. (2012). Biometrics Technology and the New Economy: A Review of theField and the Case of the United Arab Emirates. International Journal of Innovation in the Digital Economy, 3, 1–28. https://doi.org/10.4018/jide.2012100101

Alqahtani, F. H. (2017). Developing an Information Security Policy: A Case Study Approach. Procedia Computer Science, 124, 691–697. https://doi.org/10.1016/j.procs.2017.12.206

Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. International journal of social research methodology, 8(1), 19-32.

Awasthi, A., and Grzybowska, K. (2019). Handbook of research on interdisciplinary approaches to decision making for sustainable supply chains.

Baker, P. R., and Benny, D. J. (2013). The complete guide to physical security. CRC Press.

Barnes, W., Goydan, P., and Berns, M. (2019). Protecting Oil Infrastructure in an Era of

Campbell, G. (2014). The manager's handbook for business security (2nd ed.). Elsevier. Commtel Networks, C. (2020). Turnkey projects. Commtel Networks.

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.

Fennelly, L. J. (2017). Effective Physical Security (5th edition). Elsevier Science and Technology Books, Inc.

George, J. (2015). Patrol cars will now scan your face. In Emirates24|7. https://www.emirates247.com/news/emirates/patrol-cars-will-now-scan-your-face- 2015-11-01-1.608819

Harris, S. (2013). CISSP all-in-one exam guide, sixth edition. McGraw-Hill.

Hassaballah, M., and Aly, S. (2015). Face recognition: Challenges, achievements and future directions. IET Computer Vision, 9(4), 614–626. https://doi.org/10.1049/iet- cvi.2014.0084

Hilotin, J., and Pulikkal, V. (2021). UAE approves facial recognition in some key sectors: How the technology is changing our world. Gulf News. https://gulfnews.com/special-reports/uae-approves-facial-recognition-in-some-key- sectors-how-the-technology-is-changing-our-world-1.1613489780323

https://www.commtelnetworks.com/customer_references_testimonials_oil_gas.php

Hutter, D. (2016). Physical Security and Why It Is Important. SANS Institute ReadingRoom. IntechOpen. https://doi.org/10.5772/62950

Introna, L., and Nissenbaum, H. (2009). Facial Recognition Technology: A Survey of Policy and Implementation Issues. https://www.researchgate.net/publication/228275071_Facial_Recognition_Technology_A_Survey_of_Policy_and_Implementation_Issues

Journal of Information Security and Cybercrimes Research, 1(1). https://doi.org/10.26735/16587790.2018.004

Kashwani, G. A. (2017). Enhancing the Implementation of Safety Engineering Systems in Oil and Gas Construction Projects in the UAE [PhD Thesis, Heriot-Watt University]. https://www.ros.hw.ac.uk/bitstream/handle/10399/3251/KashwaniGA_0917_egis.pdf?sequence=1

Khudhair, H. Y., Jusoh, A., Mardani, A., Nor, K. M., & Streimikiene, D. (2019). Review of Scoping Studies on Service Quality, Customer Satisfaction and Customer Loyalty in the Airline Industry. Contemporary Economics, 13(4), 375-388.

Landucci, G., Khakzad, N., and Reiners, G. (2020). Physical security in the process industry (1st ed.). Elsevier.

Leeuw, K. M. M. de, and Bergstra, J. (2007). The History of Information Security: A Comprehensive Handbook. Elsevier Science.

Moses, S., and C. Rowe, D. (2016). Physical Security and Cybersecurity: Reducing Risk by Enhancing Physical Security Posture through Multi-Factor Authentication and other Techniques. International Journal for Information Security Research, 6(2). https://doi.org/10.20533/ijisr.2042.4639.2016.0077

Nasrallah, T. (2021). UAE to use facial identification in some sectors: Cabinet led by Sheikh Mohammed decides. Gulf News. https://gulfnews.com/uae/government/uae- to-use-facial-identification-in-some-sectors-cabinet-led-by-sheikh-mohammed- decides-1.1613315910160

NEC Corporation. (2017). NEC's Video Face Recognition Technology Ranks First in NIST Testing. NEC Corporation. https://www.necam.com/newsroom/pressannouncements/2017announcements/NISTRanking/

New and Emerging Threats. In BCG Global. BCG Global. https://www.bcg.com/publications/2019/protecting-oil-infrastructure-in-era-of- new-and-emerging-threats

Nilsson, N. J. (2010). The quest for artificial intelligence: A history of ideas andachievements (1st ed.). Cambridge University Press.

Pollard, M. (2020). Even mask-wearers can be ID'd, China facial recognition firm says. Reuters. https://www.reuters.com/article/us-health-coronavirus-facial-recognition-idUSKBN20W0WL

Rickli, J.-M. (2018). The Economic, Security and Military Implications of Artificial Intelligence for the Arab Gulf Countries. EDA INSIGHT. https://eda.ac.ae/docs/default-source/Publications/eda-insight_ai_en.pdf

Rouse, M. (2016). Physical Security. Search Security. https://searchsecurity.techtarget.com/definition/physical-security Routledge.

Sas, M., Hardyns, W., van Nunen, K., Reniers, G., and Ponnet, K. (2020). Measuring the security culture in organizations: A systematic overview of existing tools. Security Journal. https://doi.org/10.1057/s41284-020-00228-4

Schwarzl, C., and Weippl, E. (2011). A Systematic Empirical Analysis of Forging Fingerprints to Fool Biometric Systems. Int. J. Secur. Softw. Eng., 2(1), 40–83. https://doi.org/10.4018/jsse.2011010103

Sinha, A., Nguyen, T. H., Kar, D., Brown, M., Tambe, M., and Jiang, A. X. (2015). Fromphysical security to Cybersecurity. Journal of Cybersecurity, 1(1), 19–35. https://doi.org/10.1093/cybsec/tyv007

Stewart, J. M., Chapple, M., & Gibson, D. (2012). CISSP: Certified Information Systems Security Professional Study Guide (6th ed.). Sybex.

Swanson, C. R. (2020). Professional security management: A Strategic Guide (1st ed.).

Walton, H. (2016). Security culture: A How-to Guide for Improving Security Culture andDealing with People Risk in Your Organization (1st ed.). Routledge.

Wójcik, W., Gromaszek, K., and Junisbekov, M. (2016). Face Recognition: Issues, Methods and Alternative Applications. In S. Ramakrishnan (Ed.), Face Recognition.

Yang, W., Wang, S., Hu, J., Zheng, G., and Valli, C. (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review. Symmetry, 11(2). https://doi.org/10.3390/sym11020141

Yas, H., Alkaabi, A., Al Mansoori, H. M., Masoud, M., & Alessa, A. (2021). A scoping review research on the dynamics managing of Coronavirus disease (COVID-19). Ilkogretim Online, 20(2).

Yas, H., Jusoh, A., Abbas, A. F., Mardani, A., & Nor, K. M. (2020). A review and bibliometric analysis of service quality and customer satisfaction by using Scopus database. International Journal of Management (IJM), 11(8).

Yasseri, S. and. (2019). A Systems Engineering Approach to Physical Security of Oil and Gas Installations. International Journal of Coastal and Offshore Engineering, 3(3). https://doi.org/10.29252/ijcoe.3.3.17