Exploring the impact of advanced technologies on the physical security profession: A sociotechnical perspective*

Mia Korhonen[1] and Moufida Sadok[2*]

[1] University of Portsmouth, School of Criminology and Criminal Justice, Portsmouth, United Kingdom
[2] University of Portsmouth, School of Criminology and Criminal Justice, Portsmouth, United Kingdom

Abstract

This paper reports the results of an inquiry into physical security and the impact of advanced technologies on the perception of professionalisation. The empirical study involved 38 practitioners from a company's global physical security team, representing professionals with diverse roles, responsibilities, experiences, and backgrounds. The key findings suggest that practitioners are concerned about threats arising from emerging technologies and, more importantly, that there is a lack of governance and the necessary skills and competencies to respond to these threats. To improve preparedness and response to constantly evolving threats, this study suggests a skills-based approach grounded in a holistic framework that integrates key domains of the physical security profession.

Keywords

Physical security, professionalisation, Sociotechnical, practitioners, drones, AI

1. Introduction

The evolving security threat landscape, driven by deepening geopolitical tensions, societal polarisation, environmental risks, and the adverse outcomes of emerging technologies, requires more effective risk management and security professionalism than ever before (1). Furthermore, the increasing dependence of modern infrastructure on distributed, complex cyber-physical systems has expanded the security attack surface, requiring more proactive response and mitigation of combined cyber-physical security incidents. Mumford (1999) calls out two factors contributing to effective risk management and problem solving: a holistic approach and critical competencies of those working in organisations, ensuring that technology is deployed as a partner to human judgment [2].

These developments necessitate a comprehensive security risk assessment of the cascading impacts of advanced technologies, which are expected to significantly reshape practitioners' perspectives (3). Goto (4) argues that technology influences the construction of professional

STPIS2026: Proceedings of the 12th International Conference on Socio-Technical Perspectives in IS, September 16-17th L'Aquila, Italy
* Corresponding author.
† These authors contributed equally.
up917354@myport.ac.uk (Mia Korhonen); moufida.sadok@port.ac.uk (Moufida Sadok)
0009-0001-4892-8145 (Mia Korhonen); 0000-0003-2981-6516 (Moufida Sadok)
© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-4334/paper16.pdf

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2026-11-19

identity by interpreting it as a new constellation of institutional logic for professionals. This finding is particularly interesting for physical security, which relies heavily on technology and is expected to be further shaped by intelligent technologies (5, 6). There has been minimal research on how physical security practitioners perceive the role of technology in their work. As Josifovski et al. (2025) demonstrate in their research, the socio-technical mismatch can erode organisational stability [7]. Therefore, they argue that pure technocentric implementation often floundered because it ignores human and organisational context [7]. Technological frameworks must not be viewed strictly as tools for functional efficiency but rather as collaborative platforms that require joint optimisation with human literacy and specialised governance skills.

Considering that technology can harmonise managerialism and professionalism, it is important to understand how the profession embraces and represents this evolution (4). This research focuses mainly on addressing the question: "How would the physical security sector need to adapt to keep pace with the evolving threat landscape?" It involves interviews and observations with 38 practitioners and explores perceptions of professionalism, the occupation's current standing, and its prospects. While the study reflects perceptions globally, the participants represent a limited group, as they are all recruited from one company. Furthermore, this may result in specific topics, such as the relevance of AI, appearing more prominently and may reflect the company's industry focus. Conducting research with participants from diverse businesses or companies may yield different results. Therefore, it is essential to acknowledge that the findings of this study are not intended for generalisation. As exploratory research, this study provides insight into how practitioners perceive their roles and professionalism.

This paper argues that integrating emerging technologies to enhance security measures is both inevitable and essential. These technologies have a pivotal role in contemporary security practices. It is imperative to further investigate the impact of these technologies, particularly the role of governing frameworks as an interdependent dimension of professional capability. Moreover, further research is needed to assess the risks associated with the application and development of emerging technologies. Such threats encompass misinformation, disinformation, and malicious use of artificial intelligence. Currently, there is a paucity of research on equipping security professionals to navigate these developments, thereby enabling them to effectively assess and mitigate the associated risks in their practice. This study suggests that institutionalising governance for physical security across organisational sectors provides a clear entry point for learning and applying technical and other skills.

The remainder of the paper is organised as follows. The next section reviews relevant literature on debates surrounding physical security professionalisation and the potential impact of advanced technologies on the industry. Section three presents the research design. Section four presents the key findings.

2. Background

Traditionally, two elements have shaped the definition of physical security: protection and technical aspects. Physical security is frequently referred to as security engineering (8), in which people, procedures and equipment are used to protect assets [9, 10, 11]. The combination of people and technology for protection forms a solid foundation for physical security to embrace the challenges with advanced technologies. The development of

advanced technologies might, however, highlight the need for the human element in protection; not all responsibilities within physical security are technical or technology-related. As Baxter and Sommerville (2011) state, the failure to understand and implement socio-technical systems design increases the risk that systems will not contribute as expected to the goals of the organisation [12].

Baxter and Sommerville (2011) further argue that socio-technical systems design contributes to organisational structures, business processes, and technical systems [12]. Physical security includes responsibilities related to the operational dimensions of organisations, typically involving duties performed by security officers, overseen by physical security managers, and extending to the Chief Security Officer (CSO). These responsibilities encompass areas other than technical functions, such as risk management, crisis management, and budgetary oversight (13, 14). While these roles and responsibilities are frequently discussed in the context of corporate security, they are similarly represented in the physical security domain. Treating physical security as an isolated technical function ignores the dependency on the organisations where physical security operates. Different cultures as part of the organisations have distinct understandings of what security entails [15]. As Bednar and Welch (2005) argue, information systems and organisational processes cannot be decoupled from their unique contextual dependencies. Defining physical security purely through its technical components overlooks how security practices are structurally shaped by, and integrated into, wider organisational changes and human behaviours [16]. As Dalton (17) established, security should move beyond its somewhat limited perspective, focusing on either the physical or the corporate era, and instead consider the total asset protection paradigm. The consideration of organisational process advances strategic thinking and the move from individual thinking to broader, systematic thinking [16]. Alter (2015) suggests further that since most of the modern businesses are less hierarchical and they operate in a fast-moving business world; new thinking and approaches are needed [18]. Alter introduced 'work system lenses' where human participants, operational processes and technologies are evaluated as a single, dynamic activity. Applying these lenses would allow physical security to reframe itself as an integrated work system and prevent further functional silos.

Humans and human behaviour pose considerable challenges in security (19, 20, 21). Physical security, which focuses on protection measures involving human behaviour, will face limitations in the digital age, where cyber threats are pervasive (19). For example, the development of Artificial Intelligence (AI) and Machine Learning could support malevolent actors in enhancing social engineering attack vectors and exfiltrating valuable data (22). Similarly, Unmanned Aerial Vehicles (UAVs) can be used by malicious agents and have an economic impact, especially when carried out against critical infrastructure (21). Furthermore, the development of human-machine interaction technology, such as neurotechnological devices, is anticipated to expand the threats to organisations (23). Scholars note that investing in the inclusion of all security domains within emerging technologies and approaches is critical, as no single security strategy can provide complete protection and effective risk management (19, 24, 25, 26). As noted by Szadeczky and Bederna (2025), understanding the risks emerging from the development of advanced technologies requires judgment and critical risk-based thinking [27]. Therefore, physical

security professionals should not rely only on technical skills but equally invest in compliance and regulatory knowledge. Governance frameworks provide the strategic approach to optimise socio-technical implementation.

3. The study

A qualitative study was conducted to explore and understand practitioners' current perceptions of professionalism in physical security. The research obtained ethical approval from the University of Portsmouth in the UK. Informed by a comprehensive literature review, the interview questions were designed to elicit detailed accounts from physical security professionals concerning their skills, competencies, knowledge, and practical applications in the workplace. The research included semi-structured interviews, which facilitated probing responses and encouraged further elaboration or explanation (28).

The participants in this study were selected from a company's global physical security team, comprising professionals with diverse roles, responsibilities, experiences, and backgrounds. Interviews were conducted between April and August 2024, and the participants were recruited through the email invitations sent to physical security teams across the Americas (AMER), Asia-Pacific (APAC), Europe, the Middle East, and Africa (EMEA) regions. A total of thirty-eight professionals agreed to participate in the interviews: ten from the AMER, eight from the APAC, and 20 from the EMEA region. Among the participants, there were 11 females and 27 males. The interviews ranged in duration from 39 to 97 minutes, with an average of 61 minutes, resulting in a total of 39 hours and 6 minutes of recordings and nearly 2,000 pages of transcripts, produced using transcription functions in Teams and Microsoft Word.

Of the 38 participants, four practitioners had five or fewer years of experience in physical security. Of the 38 participants, 19 held degrees, five of which were in security-related fields. Sixteen certifications were obtained, 13 of which were security-related. A security-related degree could be, for example, a degree in security (risk) management. A security-related certification, for example, can be awarded by the American Society for Industrial Security (ASIS) or similar institutions.

The participants were prompted to share their experiences and elaborate on, for example, how technology affects their responsibilities; which areas or issues physical security should focus on to meet future needs; the main challenges for physical security; and how the physical security sector would need to adapt to keep pace with market developments. The selection of themes was by no means arbitrary; the approach aligns with what Bednar and Welch (2012) consider as critical systemic thinking (CST) in information systems [29]. Understanding complex environments of physical security requires perspectives of those practising it and, to analyse how practitioners critically evaluate their own systemic roles, responsibilities and practices. Furthermore, the design allowed a dive into those practices that are essential to the organisational function and quality, similar to what Wynn and Vallo Hult (2019) emphasise for qualitative and critical research [30].

Data obtained from the interviews were augmented with participant observations. Observations were conducted during two regular weekly community meetings among EMEA participants, and data were collected using notes and memos. These sessions were observed weekly from February 1 to August 31, 2024, except during the researcher's absences, resulting in 53 meetings being observed.

4. Key findings

The reflective thematic analysis revealed the need for bespoke, continuous training and education to equip security professionals with the skills required in the digital era. In particular, the participants acknowledged the impact of advanced technologies, for example, AI, on their work practices and emphasised the importance of better understanding of the relationship between human, organisational, and technological aspects of physical security. Lastly, similar to some other studies, this study calls for a better governance framework for physical security [27; 31; 32].

4.1. AI and physical security profession

With the increasing integration of technology into security practices, technical skills are essential. Technology adoption, specifically cloud computing and AI, is expected to depend heavily on the skills required in the 2023-2027 timeframe (33). According to the participants, technology is seen as both an enabler and a possibility. Many participants clearly stated that it is impossible to perform physical security responsibilities without the aid of technology. The data suggest that the most significant driver of change is the development of artificial intelligence (AI). Although it is a single component of advanced technologies, it represents the entire spectrum of advanced technologies in the practitioners' answers. Therefore, this broader perspective should be considered when interpreting the findings of this study. This finding aligns with other research indicating that 86% of employers expect AI and information processing to transform their businesses by 2030 (33). At the same time, adverse outcomes from AI technologies are predicted to be among the risks that increase the most over the next ten years (34). As various technology solutions and applications become more sophisticated, professionals can no longer assume the old knowledge asymmetry between them and end-users (35; 36). Therefore, technological proficiency, including digital literacy and governance, is critical for physical security practitioners.

Most participants emphasised the need for security professionals to be knowledgeable about advanced technologies, such as artificial intelligence (AI) and integrated security systems, that can enhance operational capabilities. Furthermore, the Fourth Industrial Revolution (4IR) is characterised by rapid technological advancements. Practitioners indicated that the 4IR presents new threats, such as attacks on critical infrastructure using advanced technology, aligning with previous studies (37). They also expressed concerns that the core protection function would become more challenging. Practitioners within operational domains often feel inadequately skilled in using advanced technologies. Also, they feel that physical security as an industry should consider more comprehensive integration of using advanced technology to mitigate the risks that these technologies pose. Those with experience in technological roles have witnessed improvements in the security systems designed to mitigate emerging risks. These participants seemed more confident that security technology could keep pace with future developments, mainly due to the ongoing training provided by technology companies or suppliers. Practitioners with operational responsibilities expressed concerns about learning the basics of assessing technology-driven threats and implementing the necessary measures to address them. They considered that relying solely on operational skills is insufficient to address future

challenges. The confusion between technical and social domains is natural, as the implementation of the technology does not equal with the structural integration providing cultural value [38].

The interviewees often feel they may lack the necessary skills, particularly technological savvy, in a rapidly evolving security landscape. The practitioners stated that most professional education and training is delivered through certifications offered by professional organisations. They also expressed concerns about the relevance of these certifications. Several noted that some certification exams have not been updated to reflect current practices and technologies, making them less valid for professionals. This sentiment suggests that, while certifications are valuable, they must remain relevant and aligned with industry advancements to be effective. Furthermore, the data suggests that physical security should prioritise comprehensive training programmes that cover the fundamentals of security, as well as advanced topics such as risk management, and governance. Participants emphasised the need to invest in employee training to develop the skills and knowledge practitioners need to handle complex security challenges. Indeed, as Sommerville (2015) argued, if the systems design does not consider the scale and different style of use, the systems are not effective [39]. Hence, he emphasised the importance of designing systems for the organisational purposes and implementation of governance.

However, most participants believe that technological development will not eliminate the need for human intervention, although the global survey forecasts the most significant losses, for example, in traditional security roles (33). Practitioners suggest that advanced technologies can be helpful for some responsibilities, especially in frontline roles. For example, they view technology as beneficial for detecting anomalies and, therefore, for directing physical security responses to incidents that technology has already assessed as severe. Practitioners would then further assess the level of response and determine any additional necessary measures.

The data also suggest some mistrust towards technology. Many practitioners have noted that technology often fails, for example due to outages or system malfunctions, and if an incident occurs during such a failure, it can have a devastating impact on the business. They also emphasised that technology may not be competent in making decisions in various situations: judgment and consideration of an appropriate approach or response require human assessment. While technology can also help monitor a larger number of objects or areas, and thereby reduce the likelihood of human error, the final judgment on how to prioritise risks from the monitored environment should belong to humans. According to the practitioners, utilising technology in this manner requires sufficient technical skills to evaluate, implement, and follow up on the actions and measures taken. In addition to technical skills, it requires critical thinking and risk assessment capabilities. Therefore, practitioners advocate for human input and pairing technologies with human expertise.

4.2. Security convergence

Participants stated that physical security must evolve by incorporating advanced technologies and enhancing collaboration between physical and cybersecurity. Security technology can also pose a vulnerability to businesses. An outdated network design, inadequate maintenance, and a knowledge gap increase the risk of cyberattacks through a weak physical security posture (40,

41, 6). According to the Centre for Digital Government (40), “Physical security needs to be integrated into the network security team, not viewed as an ancillary function.” Therefore, physical security should invest in continuous education, training, and certification to understand and utilise new technologies. Practitioners should be trained to utilise integrated and automated security systems, artificial intelligence, and data analytics to enhance their threat detection and response capabilities. The current modus operandi still relies heavily on manual processes, which can lead to missed signals and costly operational methods. For this to change, physical security should invest in data and analytics (6) and adopt a data-driven approach.

According to the participants, the most efficient approach to mitigating the risks arising from technological development is to converge it with cyber and information security. The data reveals a lack of convergence between cyber and physical security. Security convergence typically refers to the relationship between physical security and cybersecurity (42), although it can also encompass the relationship between information and physical security (24). Wakefield and Gips (24) further elaborated on the distinction between information security and cybersecurity concepts. Cybersecurity approaches integration from a defensive standpoint, whereas information security adopts a protective approach (43). This study employs both concepts interchangeably, depending on the context. It is noteworthy that there is no standardised adoption of convergence (44). ASIS (42) defines convergence as the seamless integration of security and risk functions, the sharing of standard practices and processes, and the organisational establishment of a unified function. Although ASIS (42) and Boakes (44) acknowledge that some approaches incorporate Enterprise Security Risk Management (ESRM), this discussion focuses on the convergence between two domains of security: physical and information security.

Acknowledging the ambiguous nature of convergence, participants were asked an open-ended question about their perception of the relationship between physical security and cybersecurity. Given the open nature of the question, participants freely described the relationship, with many spontaneously referencing their interpretation of convergence. Most participants used the term "convergence," with some proactively detailing their interpretations, while the researcher prompted others to provide more specific descriptions. Their responses characterised convergence as physical and cybersecurity being “linked,” “coexisting,” “symbiotic,” and as “a package.” This perception aligns with Boakes (2023), who views convergence from an organisational perspective [44]. Similarly, practitioners approach convergence from an organisational and cultural perspective rather than a technological one. Practitioners do not necessarily advocate operating as cybersecurity specialists; rather, physical security practitioners should possess sufficient skills and an understanding of how and where cybersecurity impacts physical security. While this study did not specifically investigate the reasons for convergence or its lack, genuine convergence appears to have remained unachieved. Nearly all participants reported experiences with limited convergence; however, most practitioners emphasised the importance of cooperation between cyber and physical security in the current challenging environment. Some participants noted a closer convergence between cybersecurity and physical security in their previous roles. However, they explained that they did not necessarily observe the same level of convergence in their current roles. The participants believed that they could not effectively perform their responsibilities without a more structured approach to convergence. Practitioners do not necessarily recommend a single security

approach (14) but rather advocate for an alliance between the two domains. Many security specialists have emphasised the importance of physical security in addressing cybersecurity threats (17, 40, 43). Participants highlighted the growing need for the convergence of physical and cybersecurity, suggesting that modern definitions of physical security must incorporate elements of cyber risk.

One of the findings discusses the role of governance. The discussions with practitioners highlighted the importance of adequate governance for physical security, which, according to them, is currently limited. Regulations such as DORA emphasise the convergence of cyber and physical security, shared governance, and integrated risk assessments, where security domains operate in an integrated manner. The need for a more structured convergence highlights the skills and knowledge that physical security practitioners should possess. However, the persistent structural and cultural silos preventing genuine security convergence cannot be resolved by technical harmonisation alone. As Wynn and Vallo Hult (2019) demonstrate, information systems are intrinsically bound to broader institutional structures, professional identities, and organisational power dynamics [30]. Security convergence must therefore be reframed as a negotiation of professional domains, where the successful integration of cyber and physical practices relies entirely on reshaping the underlying socio-political and educational architecture of the enterprise. Bringing together various stakeholders and functions involves not only the operational activities but also strategic planning and decision-making. This methodological approach can ultimately ensure a business's sustainability; however, professionals must acquire the technical skills and knowledge required for a holistic security approach to foster cyber and physical security alliances. Practitioners highlighted that adopting a holistic approach without adequate education is challenging. Most of their learning occurs in the job, and if one's job is strictly within physical security, one may never have the opportunity to learn about the other domains. They should also develop appropriate communication skills, as it often falls upon practitioners to articulate the impact of convergence on those outside the security domain.

5. Discussions

This study identified the development of AI as an example of advanced technologies and as the most significant driver of changes in physical security. AI is expected to transform the security industry, presenting both new opportunities and challenges. The data suggest that advanced technologies will increasingly impact physical security, as they pose emerging threats and risks, but could also help the industry develop its operations and practices. These findings suggest that physical security must adapt to technological advancements and integrate AI capabilities into security practices. AI is anticipated to transform the security industry, for example, through the use of drones and robotics (5). This study suggests that the physical security industry has not yet fully leveraged the potential of technology as described in the Fourth Industrial Revolution (4IR). The findings of this study support the view that significant development is necessary within the physical security industry to capitalise on the advantages of the technology introduced with the development of 4IR. For instance, the observations from this study suggest a lack of data use for identifying trends and making informed decisions, particularly at the strategic level. While the Fourth Industrial Revolution (4IR) features predictive analytics to anticipate trends and make data-driven decisions, the Fifth Industrial

Revolution (5IR), as an evolutionary phase of 4IR, builds on this by utilising real-time data and fostering a symbiotic relationship between humans and advanced technology (45). Alter (2019) notes that the data-driven approach in work system method (WSM) goes beyond the traditional approach: data analytics should enhance, rather than disrupt, the human participant's decision-making capabilities and the value within the broader work system [46]. However, as the participants work within the technological industry, the suggestions of this study might be affected by the nature of their organisation.

Historically, physical security has been recognised as an industry that has structured its operations on systems and mechanisms (8). The data revealed that technology is perceived as both an enabler and a risk, highlighting the interplay between technical and human elements. If the social and technical elements of an organisation's security approach are misaligned, it is exposed to critical flaws in overall security (47).

Furthermore, as in previous studies, the data indicate that a better understanding of the relationship between human, organisational, and technological aspects of physical security is needed (48; 49; 50). Physical security has traditionally been driven by technical solutions to safeguard assets, although security officers or guards often support it. This study aligns with the socio-technical management approach in enterprises to transition from adequate to optimal safeguarding and risk identification (47; 48). Consistent with other research, this study notes that social risks associated with integrating artificial intelligence into security technologies include privacy concerns and dependence on the cyber domain for their design and development (5; 27). For practitioners, this entails mastering governance and regulation frameworks that mitigate risks when designing and implementing security technologies that incorporate AI capabilities. As Bednar and Welch (2012) note, professionals must be equipped to analyse systemic boundaries, ethical implications and human dependencies of the technologies they deploy [29]. Individuals in operational roles must move from passive reaction to active governance because transitioning to a skills-based approach requires fostering critical systemic literacy (45]. The participants and observations from this study suggest that physical security must now, more than ever, establish itself as an integral component of the network alongside its cybersecurity, legal, and privacy counterparts. This finding is aligned, for example, with Bednar and Welch (2005), who identify and discuss contextual dependencies within organisational change [51]. Because physical and cyber security alliances are deeply intertwined with unique corporate cultures and structures, a one-size-fits-all model for security convergence is impossible. Instead, technical tools and governance frameworks must co-evolve, tailored strictly to the specific operational context of the enterprise [51].

6. Conclusion

Technological advancements, particularly those emerging from the Fourth and Fifth Industrial Revolutions, present both opportunities and challenges, necessitating swift adaptation while balancing human rights and organisational needs. The effective implementation of governance and risk management methodologies within physical security requires strong leadership, effective communication skills, and an understanding of business dynamics, positioning physical security as a critical yet evolving element within modern organisational frameworks. The findings reveal practitioners' concerns about the development of threats by emerging technologies and the lack of competencies and skills to respond to them. Hence, this study

suggests a skills-based approach to enhancing professionalism in physical security, grounded in a holistic view of the field. The findings also suggest that external factors such as rapidly advancing technology (particularly artificial intelligence), terrorism, severe malicious acts, and privacy requirements have shaped and will continue to shape the physical security environment.

The Fourth Industrial Revolution (4IR) has brought about a paradigm shift in society, marked by numerous technological breakthroughs (52). Although this revolution presents opportunities, it also poses challenges across all aspects of life, including protection. Protection, which lies at the heart of physical security, encompasses more than physical security alone; it also draws on other domains (53). Participants identified artificial intelligence (AI) as the most significant driver of change in the Fourth Industrial Revolution (4IR). They view AI as more than a technological advancement; it will transform everything, from human to organisational operations. From practitioners' perspective, AI's impact is twofold. First, AI influences the threat landscape and how security responds to evolving threats. Second, within security, information and physical security must coordinate efforts to prevent, detect, and respond to increasingly complex and uncertain security challenges (24). The two helices, the experience of systems and infrastructure and the reflection of use, are two different strands, and simply focusing on the technical strand is not sufficient; governance skills are equally important, and they facilitate the implementation [32].

This study found that technology and a continually evolving threat landscape are transforming the physical security domain from the practitioners' perspective; however, further research is needed to more effectively integrate physical security with other disciplines, such as enterprise risk management, governance, privacy, and cybersecurity.

Declaration on Generative AI

During the preparation of this work, the author(s) used [AI tool 1] in order to check grammar and spelling. After using these tool(s)/service(s), the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

References

[1] World Economic Forum (2025b). Global Risks Report. https://www.weforum.org/publications/ global-risks-report-2025/.

[2] E. Mumford (1999). Dangerous decisions: Problem solving in tomorrow's world. Kluwer Academic/Plenum Publishers.

[3] B. van den Berg, P. Hutten, R. Prins, Security and safety: An integrative perspective. In International Security Management: New Solutions to Complexity (2020) 13-27. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-42523-4

[4] M. Goto, Collective Professional Role Identity in the Age of Artificial Intelligence. Journal of Professions and Organisation, (2021) 8(1), 86–107. https://doi.org/10.1093/jpo/joab003

[5] ASIS, Artificial Intelligence in Security: Opportunities and Implications of Using Artificial Intelligence in Establishing a Secure Physical Environment. Research Report, 2021.

[6] Microsoft & Accenture, Future of Physical Security, 2018, https://www.asisonline.org/globalassets/internal/future-of-physical-security.pdf. Accessed 10 December 2024.
[7] B. Josifovski, M. Topuzovska Latkovikj, M. Borota Popovska & V. Zabijakin Chatleska (2025). Designing human-centred socio-technical systems to mitigate turnover intention: Evidence from the Macedonian IT industry. In P. Bednar, M. Rajanen, J. Kävrestad, H. Vallo Hult, A. Elbanna, P. Atanasov, & B. Josifovski (Eds.), Proceedings of STPIS 2025. CEUR-WS Vol. 4134, pp. 101–114). CEUR-WS.org
[8] M.P. Coole, D.J. Brooks, A. Minnaar, Educating the Physical Security Professional: Developing a Science-Based Curriculum, 2017, Security Journal, 31, 524-547.
[9] M.L. García, The Design and Evaluation of Physical Protection Systems: Vol. 2nd ed. Elsevier Ltd., 2008.
[10] B. Rogers, D. Palmgren, D. Giever, M.L. Garcia, Security education in the 21st century: The role of engineering. In the 2007 Annual Conference & Exposition, 2007, pp. 12–1259.
[11] ASIS International, Facilities Physical Security Measures Guideline. (GDL FPSM-2009). 218, 2009, https://www.asisonline.org/publications/sg-asis-facilities-physical-security-measures-guideline-2009-ed/
[12] G. Baxter, I. Sommerville, Socio-technical systems: From design methods to systems engineering, Interacting with Computers, Volume 23, Issue 1, January 2011, Pages 4–17.
[13] ASIS International and the Security Industry Association (SIA), Career Pathways in Security, 2018, https://www.asisonline.org/globalassets/professional-development/careers/documents/careerpathwaysguide.pdf
[14] S. McGee, An Exploration of the Roles, Skills, and Leadership Practices of the Chief Security Officer in Australasia: A Professional Perspective. Doctoral dissertation, University of Portsmouth, 2024.
[15] H. Forbes-Mewett (2018). The New Security. Basingstoke: Palgrave.
[16] P. Bednar and C. Welch (2005) IS, Process and Organisational Change and their Relationships to Contextual Dependencies. 13th European Conference on Information Systems (2005), pp.1466-1476.
[17] D.R. Dalton, Rethinking Corporate Security in the Post-9/11 Era: Issues and Strategies for Today's Global Business Community. Gulf Professional Publishing, 2003.
[18] S. Alter (2015). Sociotechnical systems through a work system lens: A possible path for reconciling system conceptualisations, business realities, and humanist values in IS development. In Proceedings of the 1st International Workshop on Socio-Technical Perspective in IS Development (STPIS 2015) (Vol. 1374, pp. 32–40).
[19] M. Hamza, U. Basheer, R. Abdul, and M. Raufi, Physical security to cybersecurity (challenges and implications in the modern digital landscape). Journal of Electrical Systems, 20, (2024), pp.692-702.
[20] Y. Yeniman, G. Ebru Akalp, S. Aytac, N. Bayram, Factors influencing information security management in small-and medium-sized enterprises: a case study from Turkey. International Journal of Information Management, 31(4),360–365, 2011.
[21] U.D. Ani, H. He, A. Tiwari, Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. J. Syst. Inf. Technol. 21 (1), (2019), 2–35.

[22] P. Wood, Socio-technical Security: User Behaviour, Profiling and Modelling and Privacy by Design. Challenges in the IoT and Smart Environments: A Practitioners' Guide to Security, Ethics and Criminal Threats, (2021), 75-91.
[23] A.M. Gielas, Soldier Enhancement through Brain–Computer Interfaces: The Risks of Changing Human Condition. The RUSI Journal, 170(1), (2025), 32-47. https://doi.org/10.1080/03071847.2025.2449894
[24] A. Wakefield, M. Gips, Professional Security in the Fourth Industrial Revolution. In The Handbook of Security, Cham: Springer International Publishing, 2022, pp. 731-750.
[25] Genetec, Exploring the path to IT and physical security convergence. [White paper], 2023, https://on24static.akamaized.net/event/45/72/31/9/rt/1/documents/resourceList1718896294370/genetecresource1718896294370.pdf
[26] A. Aleem, A. Wakefield, M. Button, Addressing the weakest link: Implementing converged security. Security Journal, 26 (2013), 236-248. https://doi.org/10.1057/sj.2013.14
[27] T. Szadeczky, Z. Bederna, Risk, regulation, and governance: evaluating artificial intelligence across diverse application scenarios: Risk, regulation, and governance. Security Journal, 38(1), 35, 2025.
[28] M. Saunders, P. Lewis and A. Thornhill, Research Methods for Business Students. (9th ed.). Pearson International, 2023.
[29] P. Bednar, & C. Welch (2012). Critical systemic thinking as a foundation for information systems research practice. Journal of Information, Communication and Ethics in Society (2012) 10 (3), 144–155.
[30] E. Wynn, H. Vallo Hult (2019), "Qualitative and Critical Research in Information Systems and Human-Computer Interaction". Foundations and Trends in Information Systems, Vol. 3 No. 1-2, pp. 1–233.
[31] B. Allen, T. Kelly, R. Loyear, A. Poole, A. Awojulu, A. Kmetetz, & M. Rakotomavo. (2018b). Security Risk Governance: A Crucial Component in Managing Security Risks. Journal of Applied Business & Economics, 20(1).
[32] L. H. Ferguson & J.D. Ramsay (2010). Development of a profession: The role of education and certification in occupational safety becoming a profession. Professional Safety, 55(10), 24–30.
[33] World Economic Forum, The Future of Jobs Report 202, 2025a, https://www.weforum.org/publications/the-future-of-jobs-report-2025/digest/
[34] World Economic Forum, Global Risks Report, 2025b, https://www.weforum.org/publications/ global-risks-report-2025/.
[35] J.O. McGinnis, R.G. Pearce, The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services. Fordham Law Review 82(6): 3041–66, 2014.
[36] D. Muzio, S. Aulakh, I. Kirkpatrick, Professional Occupations and Organisations. Cambridge: Cambridge University Press, 2020.
[37] A. Caldwell, The Context of Security Within the Fourth Industrial Revolution. International Journal of Industrial Control Systems Security (IJISS), 4(1), 2022.
[38] P. Bednar & C. Welch (2007). A double helix metaphor for use and usefulness in informing systems. Informing Science, 10, pp. 273–294.

[39] I. Sommerville (2015). Designing software for a million users: It's not about the technology (Keynote). In Proceedings of the 1st International Workshop on Socio-Technical Perspective in IS Development (STPIS 2015) (CEUR-WS.org, Vol. 1374, pp. 1–4)
[40] A Centre for Digital Government, Keep Physical Security from Opening Cybersecurity Risk. Best practices reduce the cyber vulnerabilities of cameras and access control systems. [White Paper], 2022 https://resources.genetec.com/en-whitepapers/keep-physical-security-from-opening-cybersecurity-risk#main-content
[41] Cyberday, Understanding Physical Security in Cybersecurity: Insights from ISO27001 and Best Practices. NIS2 Collection. Understanding Physical Security in Cybersecurity: Insights from ISO 27001 and Best Practices, 2024.
[42] ASIS International, The State of Security Convergence in the United States, Europe, and India, 2019, Washington, DC. ASIS Foundation.
[43] M. Gill, Thinking About the Benefits of Security, and the Barriers to Recognising Them. In The Handbook of Security, Cham: Springer International Publishing, 2022, pp. 997-1016.
[44] E. Boakes, Security Convergence: Building an evidence-based roadmap. Doctoral dissertation, University of Portsmouth, 2023.
[45] PricewaterhouseCoopers PwC, Decoding the Fifth Industrial Revolution: Moving towards a Resilient, Sustainable, and Human-Centric Future, 2024, https://www.pwc.in/assets/pdfs/decoding-the-fifth-industrial-revolution-v1.pdf
[46] S. Alter (2019). Applying socio-technical thinking in the competitive, agile, lean, data-driven world of knowledge work and smart, service-oriented, customer-centric value creation ecosystems. Complex Systems Informatics and Modelling Quarterly, (18), 1–21. RTU Journals.
[47] M. Malatji, A. Marnewick, S. von Solms, Validation of a socio-technical management process for optimising cybersecurity practices. Computers & Security, 95, 101846 (2020).
[48] S.M. Alfawaz, Information security management: a case study of an information security culture, Doctoral dissertation, Queensland University of Technology, 2011.
[49] S. Ernest Chang, C.S. Lin, (2007). Exploring organisational culture for information security management. Industrial Management & Data Systems, 107(3), 438-458.
[50] L. Coles-Kemp, Information security management: An entangled research challenge. Information Security Technical Report, 14(4), (2009), 181–185.
[51] P. Bednar and C. Welch, (2005) IS, Process and Organisational Change and their Relationships to Contextual Dependencies. 13th European Conference on Information Systems (2005), pp.1466-1476.
[52] K. Schwab, The Fourth Industrial Revolution. Penguin, 2017.
[53] E.P. Halibozek, G.L. Kovacich. The Old and New World of the Security Professional. In The manager's handbook for corporate security: establishing and managing a successful assets protection program (Second Edition) / Kovacich, G.L., Halibozek, E.P. (eds.). Butterworth-Heinemann, 2017.