An exploration into work practices of physical security professionals: A sociotechnical perspective

Mia Korhonen[1], Moufida Sadok[1]

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

Abstract

Physical security is a multifunctional practice that plays a crucial role in an evolving business environment. The ubiquitous digitization of information and the pervasive connectivity of work systems have created new challenges for physical security professionals. This research in progress focuses on developing a better understanding of key challenges faced by physical security professionals and exploring the impact of technological advancements on the physical security profession. The empirical inquiry involved 12 security professionals using semi-structured interviews and was conducted from an interpretive stance. The key findings reveal a mismatch between the perceptions of the importance of physical security and the actual practices, increasing awareness of the impact of information technologies on the profession, and mixed views around how to define a body of knowledge in physical security and how to establish its parameters.

Keywords

Physical security, sociotechnical, converged security, work practice, security professionals

1. Introduction

This work-in-progress paper describes some of the perceptions and perspectives of a small group of physical security practitioners about the challenges they face when practicing their professional responsibilities. The paper also contributes to the discussion about technology's increased impact on the physical security practitioners' roles. Further, this paper introduces physical security practitioners' views about defining a body of knowledge in physical security and establishing its parameters.

Physical security protects people, assets, and reputations in various organizations. In the constantly evolving business environment, safeguarding people, assets, and reputation should be at the core of business and organizational activities and decisions. However, only 75% of organizations report that their physical security function is well integrated as a component of resilience [1]. Physical security should be part of organizations' end-to-end risk management and resilience [1]. In 2023, a vast majority, 96%, of the organizations have experienced a disruption in their business in the past two years, and 91% have experienced at least one disruption other than the pandemic [2]. In light of these numbers, there is a need for physical security, and indeed, it is a significant industry; it is forecasted that the physical security equipment and services market will reach a worth of $500 billion by 2026 [3].

At the same time, it is acknowledged that physical security has and continues to face complex challenges, for example, due to the impact of evolving technology, economic conditions, and political difficulties [3]. Furthermore, physical security holds high trust and authority in guarding lives and valuable assets in this constantly developing landscape.

The 10th International Conference on Socio-Technical Perspectives in IS (STPIS'24) 16.-17.8.2024. Jönköping, Sweden

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)

According to ASIS [3], physical security employs over 30 million people globally in various roles. Against the anticipated growth and development of physical security as an industry, physical security practitioners should be equipped with a broad vision of requirements and responsibilities [4]. The recognition of physical security as a profession and the development of its competence framework are essential to meet the evolving security needs. Therefore, academia and practitioners need to align perspectives so that practitioners can make betterinformed decisions supported by educational tools [5].

The call for research and education programs for physical security based on accepted and validated principles was identified long ago [6]. Coole's observation [7] supports this view as he claims that physical security cannot be considered a profession until its practice is based on a consensual body of knowledge and educational standards. To increase the public's confidence in physical security as a profession, further research is needed on what forms the framework for physical security professionalism.

So far, research on security professionalization has focused mainly on a variety of domains in security. Some research has described the professional development of security consultants [8], security intelligence analysts [9], security risk management [10], and manned guards, specifically in the private sector [11]. Some research has been carried out to study professionalism among cybersecurity (or information security) professionals [12]. In addition, attempts to map the required competencies for security leaders have been carried out [13].

This paper reports initial observations of an attempt to contribute to filling this identified gap: to develop an understanding of professionalism among physical security professionals.

The structure of the paper is as follows. The first section discusses security, physical security, and professionalism, as these concepts give context for reporting the initial observations. The second section describes the research method and design. Section three presents the critical observations of the study, which illustrate areas informing the professionalization in security practices. The final section discusses the results and draws some conclusions of the study.

2. Background

The first author, working in the security industry for over twenty years, has found it difficult to pinpoint her sector or how to describe herself as a physical security professional. During her career, the researcher has engaged multiple times in discussions with her peers or other people about what security entails or who is considered a security professional. These discussions generated the idea for her research. As she started investigating the topic, the definitions of security, physical security, and security professionals seemed vague and ambiguous. This paper is part of her research exploring practitioners' perspectives on physical security professionals' competencies, skills, and knowledge.

This study approaches physical security practitioners as one group of professionals and does not make a distinction between the occupational sub-groups. The reason is that the researcher wanted to explore what professionals consider relevant competencies, skills, and knowledge. Categorizing the professionals beforehand would, in the researcher's view, limit the research and its potential contribution. This approach is also reflected in the research design. The participants represent various categories of professionals; some have more technical backgrounds and experience, whereas others come from security guard backgrounds and now work as security managers.

The following sections describe the ambiguity around the key concepts, namely security, physical security, and professionalism, as they give context for the study and initial observations reported in this paper. Before explaining physical security, it is necessary to look at its parent domain, security.

2.1. Security

Security is multidimensional in both concept and application [36]. From a security science perspective, it can be viewed as a practice area [36], and within that, security is usually divided into two main streams: traditional and non-traditional security [7]. Traditional security focuses on the sovereignty and stability of a nation and is politically and militarily managed. The nontraditional security sector, however, considers other threat typologies across the international community or within a country [7]. Some domains within non-traditional security are, for example, cyber security, personnel security, and physical security [14]. According to Brooks [7], the table in Figure 1 shows different categories of security as a domain subject.

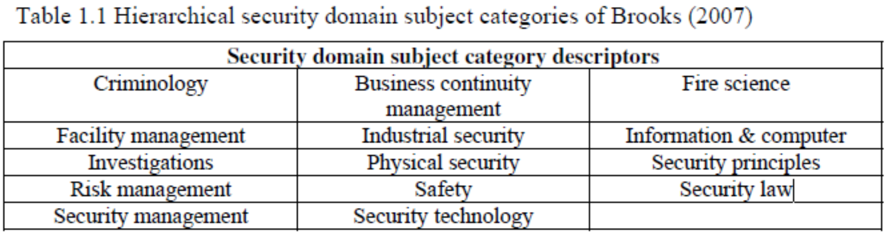

Table 1.1 Hierarchical security domain subject categories of Brooks (2007)

Security domain subject category descriptors		
Criminology	Business continuity management	Fire science
Facility management	Industrial security	Information & computer
Investigations	Physical security	Security principles
Risk management	Safety	Security law
Security management	Security technology	

Figure 1. Hierarchical categories of security domain [7].

Although the operational concept of security remains ambiguous, it also has a more philosophical context that is rooted further in the history of humanity. Fundamentally, security has been recognized as "a feeling of being safe from harm, fear, anxiety, oppression, danger, poverty, defense, protection and preservation of core values and threat to those values" [15]-[17]. For example, in Europe, the demand for security has been set out in the Stockholm program and reinforced in The European Agenda on Security, both stating that the EU aims to ensure that people live in an area of freedom, security, and justice [18]. This approach is supported by some scholars who consider security to include crime prevention, risk management, and loss prevention [19, 36]. To some, it can also include counterterrorism and business continuity functions [20].

However, several authors argue that the definition of security remains vague and inadequate [21, 17]. As Manunta [17] has called out, one of the challenges for the emerging security profession is that: "We security professionals and scholars are entering the millennium from a very flimsy position: We lack a robust and workable definition of security." Some even challenge the philosophical approach to security, claiming that it is subjective and can potentially serve as a vehicle for driving own interests [22].

The ambiguity is not only a semantic problem but also confuses the work practice of security professionals. Without a clear definition of security, how can people work on the same agenda, and how can it be determined when something is secured [22]? A more systematic approach to defining security is appropriate [16]. Only after the main elements of the security concept are identified, analyzed, and considered can it be decided which criteria should be applied in each situation [22]. The same approach should be used for sub-domains of security.

2.2. Physical security

Fundamentally, physical security is about protection; everyone protects what they consider valuable, such as their homes, belongings, and money. Physical security is described as the most fundamental aspect of protection, as a process where the layers of protective physical security measures are used to protect people, assets, and facilities [23]. As gatekeepers, physical security professionals protect employees, information, and property [24]. Some claim that physical security covers all security matters except cyber security [25].

Garcia [26] provides a slightly more detailed definition, saying that physical security is “(1) the use of people, procedures, and equipment (alone or in combination) to control access to assets or facilities; (2) the measures required for the protection of assets or facilities from espionage, theft, fraud, or sabotage by a malevolent human adversary.” Similarly, according to ASIS [27], physical security is (1) the part of security concerned with physical measures designed to safeguard people to prevent unauthorized access to equipment, facilities, materials, and documents and safeguard them against a security incident. However, ASIS [27] also adds that physical security is (2) the application of control procedures to prevent or deter attackers from accessing a facility, resource, or information. It can include physical barriers to gaining access, electronic security and alarm systems, video monitoring, staffed security, or other responses. Similarly, Coole [29] provides security engineering in his definition and states that “physical security is occupationally divided into a diverse range of distinct work roles that provide specific client-centered protective services.”

Recently, physical security has evolved towards offering new services in addition to traditional equipment and services. Technological advancements will continue to change physical security equipment and services towards a more comprehensive approach that covers energy and occupancy usage of facilities [3].

The physical security channel described by ASIS [3] demonstrates the complexity of the physical security industry. It confirms that physical security has developed from its traditional definition of gates, guards, and guns, 3Gs [14]:

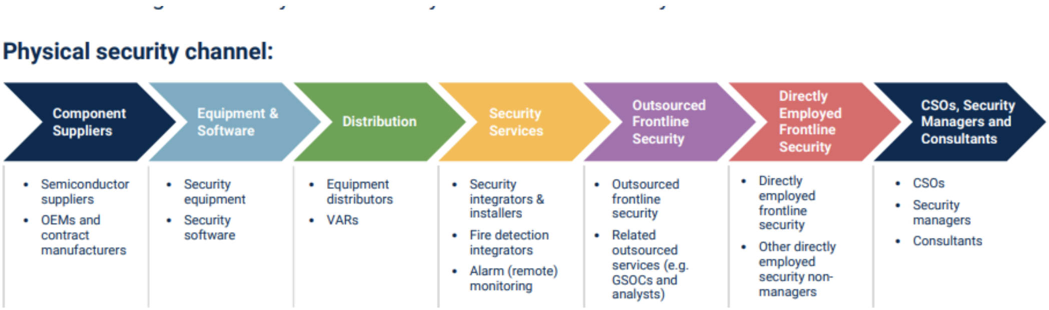
Physical security channel:
Component Suppliers
Equipment & Software
Distribution
Security Services
Outsourced Frontline Security
Directly Employed Frontline Security
CSOs, Security Managers and Consultants
Semiconductor suppliers
OEMs and contract manufacturers
Security equipment
Security software
Equipment distributors
VARs
Security integrators & installers
Fire detection integrators
Alarm (remote) monitoring
Outsourced frontline security
Related outsourced services (e.g. GSOCs and analysts)
Directly employed frontline security
Other directly employed security non-managers
CSOs
Security managers
Consultants

Figure 2. Physical security channel described by ASIS [3]

It seems that significant emphasis is placed on prevention and protection in the definition of physical security. There are, on the other hand, views that consider physical security expanding its scope beyond this. For example, Rogers et al. [28] consider physical security as using people and systems to mitigate and respond to or address the problem. Similarly, Talbot & Jakeman [14] state that a physical security system must be able to assess, mitigate, delay, and respond to a suspected physical breach of security. Coole [29] further expands the view by stating that physical security is one of the professions that “examines and treats complex threat typologies across an array of societal security concerns.”

The discussion above demonstrates the complexity of physical security responsibilities. The following section will discuss security and physical security professionalism in detail.

2.3. Professionalism

Most scholars believe that security and physical security as its sub-domain lack the profession's status [7, 6]. Professional status is essential for any discipline as it enhances the development of the scientific foundation and its basic concepts and sets the standard for the industry through the framework of accountability and vision. Furthermore, it reduces the risk of discipline being driven by emotions and subjective interests [17].

Many occupations pursue professional status; however, only a few succeed [30]. While some occupations may wish to seek the status as a profession, for many occupations, the recognition of a profession has to do with responsibility and accountability; the professional is expected to hold a certain degree of knowledge, skills, competence, and dignity to address their respective area of expertise. The emphasis is usually on knowledge, expertise, and higher education [31]. Thus, professionalism also comes with responsibility; the public's expectations of those recognized as professionals are higher. Interestingly, professionalism is not something an occupation can declare; it must be earned by the public [30].

A practical overall security approach requires a holistic approach. Regardless of size, status, environment, or business purpose, all organizations must consider risks and ways to mitigate them. Globalization, easy access to information 24/7, worldwide political and cultural conflicts, and increased immigration and diversity have impacted the threat paradigm of physical security [32, 33]. New, artificial risks have emerged from these developments, reshaping the perspective on these risks [34]. These new threats and business realities require better identification and management of security risks. This also poses demands for security professionals. As a profession, physical security must advance and develop professionalism to respond to emerging threats in different landscapes.

Moreover, the development of professionalism is essential for physical security due to an increased privatization of the security sector. For example, in the EU, an increasing number of tasks traditionally associated with state-provided security services are now provided by private security, including prominent public places and critical national infrastructure [18]. Hallcrest's [35] report called out the need for the security industry to develop, discuss, and promote its standards in the wave of privatization.

Some institutions, such as the American Society for Industrial Security (ASIS), have attempted to launch initiatives to engage with the academic world and leverage security professionalization. The characteristics of professionalism include, for example, generally accepted qualifications, a code of ethics, an academic base meaning corpus of literature, self-regulation, and governing standards [20]. Although the attempts to professionalize physical security (and security overall) are ongoing, the success is limited [10]. Garcia [6] has called after research and education programs based on accepted and validated principles. Coole's observation [7] supports this view as he claims that physical security cannot be considered a profession until its practice is based on a consensual body of knowledge and educational standards. To increase the public's confidence in security as a profession, it is crucial to establish the characteristics of the profession through academic research [7].

3. Research method

This study draws on a qualitative approach by using semi-structured interviews, observations, and thematic analysis to collect and analyze the data. The first phase of the study included a systematic literature review. The review used a systematic search strategy from databases (EBSCO Discovery, Web of Knowledge, JSTOR, and Google Scholar) using the following keywords and their combinations: security, physical security, skills, knowledge, and competence. Through this search, the key authors and their work were identified. This literature search supported formulating the interview questions for the second research phase to collect data through semistructured interviews. The second phase also included observations in the Microsoft Cloud Operations and Innovations (CO+I) physical security professionals' community.

The 12 semi-structured interviews aimed to elicit physical security professionals' accounts of their skills, competencies, and knowledge and how they enact those in their work. The participants were sampled and recruited through a gatekeeper from the Microsoft Cloud Operations and Innovations (CO+I) Physical Security team in Europe, the Middle East, and Africa.

The participants were recruited independently for both interviews and observations. Therefore, not all participants necessarily participated consecutively in both phases of the research. The interviews were conducted with 12 participants, 20 of whom consented to participation through observations. For interviews, each participant was interviewed at least once, most of them twice, over three to four months, and each interview lasted approximately one hour.

The data from observations was collected through the researcher's overt role. As the researcher is an insider in the Microsoft Cloud Operations and Innovations (CO+I) physical security professionals' community, she was able to observe the community and collect data through observations. The role and purpose of observation were shared with the team members. The observation data was collected anonymously so that the data could not be linked to any individual participant.

The observations were gathered in two weekly community meetings and recorded by writing notes and memos. The observations were recorded in both calls between 1 February and 31 May 2024 every week, except when the researcher was not participating in the calls herself.

The interviews were transcribed, and together with observation notes, the researcher organized them in a qualitative data analysis platform for coding. The researcher began the process by familiarizing herself with the data and identifying several points of interest. Through notetaking, the researcher captured ideas of patterns and meanings, which helped to cluster codes [37]. Notetaking also helped the researcher to reflect on her position as an insider of the community, and it was a conscious decision from the researcher first to stay as close to the data as possible and approach the data through semantic orientation. It was also essential to be able to give a voice to the participants. Therefore, the initial rounds of coding generated a significant number of codes, some broader and some very specific. However, with the help of the familiarization notes, the researcher was able to start combining codes, as some of the codes often captured micro differences between codes. The further the researcher coded, the more her approach sifted towards latent orientation as she started to look deeper into the meanings of codes. For this paper, through this inductive process, the three main groups of codes were selected: technology as an enabler and possibility, physical security as an undervalued core function or chameleon, and education as a tailored necessity.

4. Key findings

The findings reported in this paper are the ones the researcher interpreted as the most significant during the analysis. It is essential to highlight that the study is ongoing, and the researcher is still exploring the codes and establishing the themes. Therefore, this paper reflects the work in progress, not the final themes of the research.

4.1. Technology: possibility and enabler

According to the participants, technology is seen both as an enabler and a possibility. In many responses, it was clearly stated that it is not possible to perform physical security responsibilities without technology. For example, one of the participants stated that they or physical security overall could not do their job without technology*: "Technology plays a significant role in my daily work starting from that I am working on laptop, attending meetings online which include local and remote teams, using IT systems for raising tickets for requests, recommendations for changes, just to mention some examples. Technology is an integral part of my work; without it, I would be limited and unable to work as part of a regional/global team. In addition, technology also plays a significant part in security in general, considering the systems that security uses, such as access* *control, CCTV, etc., which serve a higher level of security instead of relying only on the human workforce doing manual work."*

Technology is also seen as a possibility as it is expected that, for example, AI will impact physical security and how it will be performed. Although technology, specifically AI, can bring emerging threats, it is perceived as a positive development among practitioners: *"...far away in the last ten years, and I would predict that in the next ten years, we would see a lot more of that AI in place and let's say fewer humans on site. I think in the end, this human will be there too. The AI has identified that there is a problem here: that humans will still need to intervene and do the final calculation based on common sense."*

Many participants also stated that physical security will always require human aspects and contributions no matter how technology develops. Some practitioners consider physical security not fully utilizing technology, but there is more potential for physical security as an industry to use it to perform its responsibilities more efficiently.

4.2. Physical security: undervalued core function or chameleon?

According to many participants, physical security suffers from an undervalued perception. Many respondents described physical security as "rather a cost than an asset." The challenge seems to be that when things go well, and there is no disruption to the business, companies or organizations have difficulties understanding what added value physical security as a business function brings. However, at the same time, if something goes wrong, the criticality towards physical security is demonstrated. One of the participants illustrates this point by saying, "...people question why we have security, but when something goes wrong and there's no security, then it's like, *where was the security?"*

Often, physical security practitioners feel that they are there to make the lives of others difficult, set up rules, and challenge people when the rules are not complied with. This gives a negative dimension to physical security, and as participants stated, it is hard to work in a positive vacuum with other business functions. This view came across primarily through participant observations where people had an opportunity to discuss their work among their peers [the quote is a free interpretation note by the researcher]: "How to best position physical security as a key stakeholder in daily operations and emphasize *the mission."* At the same time, as some respondents noted, physical security as an industry has failed to showcase its importance and sell the value of physical security to business executives.

Physical security has experienced changes within the past couple of decades, mainly due to significant geopolitical incidents such as 9/11 and malicious acts across the globe. Quite a few participants mentioned that some responsibilities have been transferred from governmental security services, such as police, to private physical security as there are insufficient police and resources to maintain security. Therefore, the participants believe physical security is a growing industry that can meet constantly changing threats and challenges. Interestingly, this seems to conflict with the view that other businesses do not appear to value or prioritize physical security, at least not until something goes wrong. Despite the overall negative perception, the practitioners feel an apparent demand for physical security services could increase the profession's contribution to organizational continuity and resilience.

4.3. Education: tailored necessity

Respondents reported that having a one-size-fits-all education for physical security is challenging. Physical security is considered an industry with many tasks and responsibilities. At its current state, it would be challenging to determine what basic education should contain. However, many participants emphasized that physical security as an industry needs a basic education mainly for two reasons.

The first reason is about the brand and how physical security is perceived. Some participants noted that without self-respect as a professional, it is difficult to expect others to appreciate physical security: *"…is we have to value ourselves more in what we do and what we deliver and sell that better to our customers. We have to pay people more to attract the right quality people and get that retention within the teams."* According to some participants, better self-respect is directly linked with appropriate education. One participant affirmed, *"So more investment in education, you know, educational courses, professional qualifications, more structure and then in a professional way. So, they actually hold their value."*

Secondly, the lack of a career path was seen as a challenge for the industry to lift its image. Currently, most of the respondents consider physical security to be an entry-level job which many choose to earn their living: *"People will often, umm, look at security positions like a like a somewhere that they can just, you know, make some money to move forward to another position, and they don't see it as a role for life, and they don't see it as a profession."* Once you enter the industry, navigating the roles is difficult because there is an apparent lack of career path: *"We also need to build out structured career paths so people can go from the bottom to the top, and it's detailed."* Since there is a lack of basic education, there is also no further education within the industry to, for example, provide the necessary skills for managerial roles. Also, the lack of an established framework for soft skills was seen as a challenge, as physical security is very much people's business.

5. Discussion and Conclusion

This work-in-progress aimed to explore some of the perspectives of professionalism components by physical security practitioners. There is little research on what physical security practitioners consider the core elements of their professionalism, and this paper contributes to that discussion.

The initial key finding of this study mentions the applicability of technology as one of the critical elements of physical security professionalism. Although it is recognized how much security has evolved [38], there seems to be a view among the practitioners that the potential of technology could be better converged to support physical security responsibilities. As Sadok et al. [39] have suggested, companies would benefit from adopting a socio-technical approach to promote a culture of security awareness. The Fourth Industrial Revolution (4IR) calls for fundamental rethinking for professions and physical security professionals confronting the gap, for example, towards cyber security and artificial intelligence, which is critical [38]. Considering how fast technology has developed, it is slightly surprising to learn from the practitioners that there is still such a gap in how technology has been harnessed in their practice. Adaption has been identified as the priority of professionalization and a source of future advantage [38]. Physical security as an industry would need to investigate how to close the gap. This would support the further development of its professionalization as it would improve the industry's resilience [38].

Based on the primary findings, there seems to be a mismatch between the perception of the importance of physical security and the actual work practice. Practitioners consider their work a critical industry but expressed concern that physical security is not prioritized in practice. Companies and organizations across the globe spend money on security systems and human resources [3]. Still, as demonstrated by participants in this study, physical security is often perceived rather as a cost than an asset. This unflattering perception by executives and senior management has been well-recognized [40, 41]. As participants noted, physical security is a widely abused concept that has been a subject of questionable marketing, blame, and liability [17]. As participants mentioned, security has failed to brand itself properly, which poses challenges to professionalizing the whole security industry, including physical security. Interestingly, within 25 years, physical security has not been able to change the fact that expectations put on physical security cannot be realistically met [17].

Among practitioners, however, there is a strong consensus that physical security has much to bring to organizations and that physical security will remain a critical industry, especially considering the ongoing privatization of physical security responsibilities [41].

Lastly, the participants stated that physical security requires an established education; however, they have mixed views on how a base education could be achieved, as physical security has many roles and responsibilities. Similarly, Wakefield [41] notes that the broader disciplinary base would be hard to place for security as it fulfills various functions. Further, it has been argued that more established disciplines, such as medicine and law, have been able to demonstrate their body of knowledge. However, they have a variety of functions within them, too [36]. Wakefield [41] suggests that security has not been able to establish its body of knowledge because there is no clear ownership. It remains unclear who should drive the development of that. Indeed, the observations of this study indicate similarly that it is hard to pinpoint which institutions or associations would have that responsibility.

The primary findings from this study support the view that physical security, and security as its parent domain, still need to work on establishing the professional framework. This will be critical as the industry can be adaptive and resilient through the professional framework for all its challenges in the contemporary threat landscape.

References

[1] PwC 2021; Physical security URL: https://www.pwc.com/gx/en/issues/crisis-solutions/business-resilience/physical-security.html

[2] PwC 2023: Global crisis and resilience survey 2023. URL: https://www.pwc.com/gx/en/crisis/pwc-global-crisis-resilience-survey-2023.pdf

[3] American Society for Industrial Security, ASIS (2024): Complexities in the Global Security Market 2024-2026. URL: https://www.asisonline.org/publications--resources/asis-sia-joint-economic-study/

[4] Muller, E.R. Trends on Security, Safety and Criminal Justice in the Netherlands, in Jacobs, G., Suojanen, I., E. Horton, K. & Saskia Bayerl, P. (Eds). International Security Management: New Solutions to Complexity. Springer, 2021.

[5] Jacobs, G., Suojanen, I., E. Horton, K. & Saskia Bayerl, P. Towards Sustainable Solutions in International Security Management—An Introduction, in Jacobs, G., Suojanen, I., E. Horton, K. & Saskia Bayerl, P. (Eds). International Security Management: New Solutions to Complexity. Springer, 2021.

[6] Garcia, M.L. Personal Opinion: Raising the Bar for Security Professionals. Security Journal, 13, (2000) 79-81.

[7] Coole, M. P. Physical Security Professional's Body of Knowledge: a cultural domain analysis of physical security's knowledge structure. Doctoral dissertation, Curtin University, 2015. [8]

Scott, D. C. Transnational security consulting: UK practitioner perspectives. Doctoral dissertation, University of Portsmouth, 2020.

[9] Duvenage, M. A. The Professional Identity of Security Risk Intelligence Analysts in the Private Sector: An International Perspective. Doctoral dissertation, University of Portsmouth, 2021.

[10] Hasenstab, A. N. The thoughtful security practitioner: Exploring reflective practice in security risk management. Doctoral dissertation, University of Portsmouth, 2017.

[11] Garrett, D. Private security career paths: Establishing the foundations of a structured progression model for the manned guarding sector. Doctoral dissertation, University of Portsmouth, 2016.

[12] Patton, Helen E. Navigating the Cybersecurity Career Path. Wiley, 2022.

[13] Mathews, T. J. Professional certification: Does the security industry need a new yardstick? New Jersey City University, 2015.

[14] Talbot, J., Jakeman, M., Security risk management body of knowledge. Wiley, 2009.

[15] Afolabi, Muyiwa, Concept of Security, in: Kunle Ajayi (Ed.), Readings in Intelligence and Security Studies, Intelligence and Security Studies Programme, ABUAD, 2015, pp.1 – 11. [16] Fischer, R. J. (2014). Introduction to security / Robert Fischer, Edward Halibozek, David Walters. Elsevier.

[17] Manunta, G. Towards a security science through a specific theory and methodology, Doctoral dissertation, University of Leicester, 1997.

[18] Button, M., & Stiernstedt, P. The evolution of security industry regulation in the European Union. International Journal of Comparative and Applied Criminal Justice, 41(4), (2017) 245-257.

[19] Brooks, D. J., What is security: Definition through knowledge categorization. Security Journal, 23, (2010) 225-239.

[20] Borodzicz, E. P., & Gibson, S. D., Corporate Security Education: Towards Meeting the Challenge. Security Journal, 19(3), (2006) 180–195.

[21] Griffiths, M., Brooks, D., Corkill, J., Defining the Security Professional: Definition through a Body of Knowledge, in: Proceedings of 3rd Australian Security and Intelligence Conference, Edith Cowan University, Perth Western Australia, 30th November 2010. pp. 44-52. doi: 10.4225/75/579ed9e4099cd.

[22] Manunta, G., What is Security? Security Journal, 12, (1999) 57-66.

[23] Kovavitch & Halibozek, Physical Security, in Fennelly, L. J. (Ed.). Effective physical security. Elsevier Science & Technology, 2012, pp. 339-353.

[24] Baker P.R., Benny D.J., The Complete Guide to Physical Security RC Press; 2013.

[25] Landucci G., Khakzad, N., Genserik R., Physical Security in the Process Industry: Theory with Applications. Elsevier, 2020.

[26] Garcia, M. L., The Design and Evaluation of Physical Protection Systems: Vol. 2nd ed. Elsevier Ltd., 2008.

[27] ASIS: A Comprehensive Glossary of Terms for Security Industry. A resource for security professionals, 2020. URL: https://www.asisonline.org/globalassets/professional-development/careers/career-resources/wis---glossary-of-terms-for-the-security-industry..pdf?_t_id=8yEa3b8FuoYiSDOGiKOD8A%3d%3d&_t_uuid=nccZsFMORq2t7if185Q7Iw&_t_q=glossary&_t_tags=language%3aen%2csiteid%3ab1140b07-9e31-4808-809a-878911c7f3f1%2candquerymatch&_t_hit.id=ASIS_Models_Media_Assets/_1720fa95-d796-40d8-82e5-e5b14df1f5ea&_t_hit.pos=1

[28] Rogers, B., Palmgren, D., Giever, D., & Garcia, M. L., Security education in the 21st century: The role of engineering, in: Proceedings of ASEE Annual Conference and Exposition, 2007.

[29] Coole, M. P., Brooks, D. J., & Minnaar, A., The physical security professional: Mapping a body of knowledge. Security Journal, 30(4), 1169-1197, 2017.

[30] Wilensky, H. L. The professionalization of everyone? American journal of sociology, 70(2), 137-158, 1964.

[31] Saks, Mike, Defining a Profession: The Role of Knowledge and Expertise. Professions and Professionalism, 2(1). doi.org/10.7577/pp.v2i1.151, 2012.

[32] Tyson, D., Security convergence: managing enterprise security risk. Elsevier/Butterworth-Heinemann, 2007.

[33] Masys, A. (Ed.) Security by Design: Innovative Perspectives on Complex Problems. Springer, 2018.

[34] Van den Berg, B., Hutten, P., & Prins, R., Security and Safety: An Integrative Perspective, in Jacobs, G., Suojanen, I., E. Horton, K. & Saskia Bayerl, P. (Eds). International Security Management: New Solutions to Complexity. Springer, 2021.

[35] Cunningham, W. C. Private security trends, 1970 to 2000: the Hallcrest report II / William C. Cunningham, John J. Strauchs, Clifford W. Van Meter. Butterworth-Heinemann, 1990.

[36] Smith, C.L., Brooks, D.J., Security science: the theory and practice of security, Elsevier, BH, 2013.

[37] Braun, V., Clarke, V., Thematic analysis: a practical guide, SAGE, 2022.

[38] Wakefield, A. & Gips, M., Professional Security in Fourth Industrial Revolution. In: Gill, Martin, ed. The Handbook of Security. Cham: Springer International Publishing AG, 2022. [39] Sadok, M., Welch, C. & Bednar, P. A socio-technical perspective to counter cyber-enabled industrial espionage. Security Journal 33, 27–42, 2020. doi.org/10.1057/s41284-019-00198-2.

[40] ASIS: Current State of Security Risk Management, 2021. URL: https://www.asisonline.org/globalassets/publications-and-resources/security-issues-research/2023-24/security-risk-management/asis-security-risk-management-research-report.pdf

[41] Wakefield, A. Where Next for the Professionalization of Security? In: Gill, Martin, ed. The Handbook of Security. London: Palgrave Macmillan UK, 2014.