Journal of Integrated Security Science

An integrative conceptual framework for physical security culture in organisations

Karolien van Nunen[1,2,3,*], Marlies Sas[2,3], Genserik Reniers[3,4] , Geert Vierendeels[5], Koen Ponnet[6], Wim Hardyns[7]

1. *Research Chair Vandeputte, University of Antwerp, Belgium*
2. *Law Enforcement, Faculty of Law, University of Antwerp, Belgium*
3. *Antwerp Research Group on Safety and Security (ARGoSS), Department of Engineering Management (ENM), Faculty of Applied Economics, University of Antwerp, Belgium*
4. *Safety and Security Science, Faculty of Technology, Policy and Management, Delft University of Technology, The Netherland*
5. *Department Health, Safety & Environment, Solvay, Belgium*
6. *Department of Communication Sciences, IMEC-MICT, Ghent University, Belgium*
7. *Department of Criminology, Criminal Law and Social Law, Ghent University, Belgium*

A conceptual framework for physical security culture in organisations is proposed, based on the integrative model of safety culture, as developed by Vierendeels et al. (2018). The proposed conceptual framework for physical security culture has the advantage that it brings security threats, technique, organisation and human aspects together in a coherent, integrative and related way. The framework includes five main domains of security culture, being (1) an observable technological domain, (2) an observable organisational domain, (3) an observable human domain, (4) a non-observable organisational domain or perceptual domain, and (5) a non-observable human domain or psychological domain. These five main domains can be further divided into several more specific sub-domains of security culture. At their turn, these sub-domains can be translated into measurable security results, being (1) observable security outcomes, (2) the security climate of an organisation or the shared perceptions on security, and (3) the individual intention to behave secure or insecure. The aim of the framework is to take all security-related aspects into account – based on the specific security threats to which an organisation is exposed – leading to a pro-active approach of the physical security of organisations. The framework provides specific points of departure to make the security culture measurable, and by extension controllable.

Keywords: Security culture; organisational culture; physical security; integrated model; security management; measuring security

* Corresponding author.
Email address: Karolien.vannunen@uantwerpen.be

ISSN: 2468-4546

1. Introduction

The field of academic research in the domain of security is relatively new. Only since the beginning of this century, attention for security has been translated into scientific research, with a huge boost in studies since 9/11. From then on, more and more security initiatives have been emerged in both science and practice. Due to the relative young status of security research, conceptual frameworks, theories, and models are still fully developing. An advantage in this ongoing development process, is the resemblance of security with safety, causing that inspiration for security research can be found in the field of safety research, of which the latter has a longer academic history.

In this paper, a conceptual framework for physical security culture in organisations is proposed, based on the integrative model of safety culture, as developed by Vierendeels et al. (2018). The safety culture model of Vierendeels et al. (2018) is called The Egg Aggregated Model (TEAM) of safety culture, and is developed based on an extensive review of literature regarding existing studies and models with respect to safety.

2. Main resemblances and differences between safety and security

For a long time, security and safety were seen as independent from each other. Though, more recent research illustrates that there arises synergy when safety and security measures are considered jointly. Much can be learned from adopting the knowledge of the one discipline to the other and vice versa (Kria et al., 2015).

The main resemblance between safety and security is the focus on preventing undesirable events such as injury to people, material damage and environmental damage. The main difference is the origin of these undesirable events, being *unintentional* in the field of safety, and *intentional* in the field of security.

This difference in origin leads to an important distinction in the desired degree of transparency. In the field of safety, a high level of transparency – both within and outside organisations – is required in order to optimally prevent undesirable safety events and in order to optimally come to insights and learn from each other. However, in the field of security, this transparency is also needed, but only within trusted communities, for instance within a single plant or between multiple plants of the same organisation. Outside these trusted communities, the level of transparency should be curtailed in order to optimally prevent undesirable security events and to protect (sensitive) information. This can be clarified by, for example, storage tanks of chemical products. Safety-wise, the characteristics of the stored chemicals should be easily retrievable in case of for instance a leak or a fire. However, security-wise, the retrievability of the chemical characteristics makes it easier to choose a target in case of for instance theft or a terrorist attack. Therefore, this information should only be shared within the trusted community, for instance with the nearest fire department.

Another distinction relates to the difference between *risks* in the domain of safety, and *threats* in the field of security. Safety risks are predominantly rooted inside the organisation, whereas security threats are mostly rooted outside of the organisation. Safety risks are often well-known by the organisation, as the accident scenarios are inherently

linked to the specific characteristics of the organisation. However, looking at security, it is more difficult to fully cover the specific threats to which an organisation is exposed, as this could cover a wide spectrum of possible scenarios that are influenced by aspects out of the control or knowledge of an organisation (Jore, 2017).

A noteworthy resemblance is that both safety and security can be viewed as a part of the overall organisational culture (Hopkins, 2006; Connolly, 2000). This implies that both safety and security should be integrated in other corporate processes. Doing so, in order to be as efficient and effective as possible, both safety and security should be assessed in an integrative, holistic way. In other words, continuous attention is needed for both the safety culture and the security culture of an organisation.

3. The need for a proactive and integrative approach of security culture

Organisations – and even governances – are approaching their security in a predominantly reactive manner which is incident-driven, instead of using a more proactive approach (Ruighaver et al., 2007). Also, based on the literature, it can be concluded that security research often lacks an integrative approach. After all, it are mainly the technological security aspects that receive attention. It is only in the last decade that the concept of security culture gains interest from researchers and business leaders, with a dominant position of information/cyber security. There is nearly no reference to other types of security issues. However, in analogy with safety culture, a proactive and holistic approach is needed when addressing the security culture of an organisation.

As elaborated in the safety culture model of Vierendeels et al. (2018), safety culture consists of three main domains, being a technological, an organisational and a human domain. This approach can be extended to the field of security culture, where security culture consists of three main domains:

(1) A technological domain, which comprises aspects regarding the present security technology, material and equipment present in the company.
(2) An organisational domain, which comprises aspects such as the security management, the company security policy, and the resources available for security.
(3) A human domain, which comprises aspects such as knowledge, attitudes, assumptions, decisions, and actions of individuals regarding security.

Both the organisational and the human domain are manifested at two levels:

(1) Firstly, there are the tangible, observable aspects regarding security. These are the aspects that are observable when walking around in the company. This concerns, for instance, the security behaviour of employees, or the security rules, procedures, instructions, etc. that can be consulted in documents of the company.
(2) Secondly, there are the less tangible, non-observable aspects. These are the aspects that cannot be observed by walking around in a company. This concerns, for instance, what employees think of the level of security in the company, or the attitude they have towards security.

The technological domain consists only of observable aspects. This structure leads to five domains, as can be seen in Figure 1, which together form the physical security culture of an organisation. The five domains can be further divided into several sub-domains, which are represented as the white boxes in Figure 1. Important are the arrows in the model, which symbolise that all the different domains of the physical security culture are related in a cyclic way.

The grey boxes in the conceptual model represent the security results. In case of the three observable domains, the several sub-domains result in observable security outcomes. In case of the non-observable organisational domain or the perceptual domain, the several sub-domains result in the security climate of an organisation, being the shared perceptions on security. In case of the non-observable human domain or the psychological domain, the several sub-domains result in the individual intention to behave secure or insecure.

The security culture of a specific organisation is influenced by external factors such as the level of technological development of a country or a region, the socio-economic status of a country or a region, the policies, regulations and legislations of a country or a region, the national culture, etcetera. In addition, the security culture of an organisation is inextricably linked to the security threats to which a specific organisation is exposed to. In other words, the entire security culture of an organisation – security results included – is influenced by the specific security threats of the organisation. For instance, in the financial sector, the security threats of espionage, fraud and theft are more prominent than for instance in the chemical sector where the security threats of terrorism and activism are more prominent. The presence of these possible security threats influence the entire development and rollout of the security culture of the organisation.

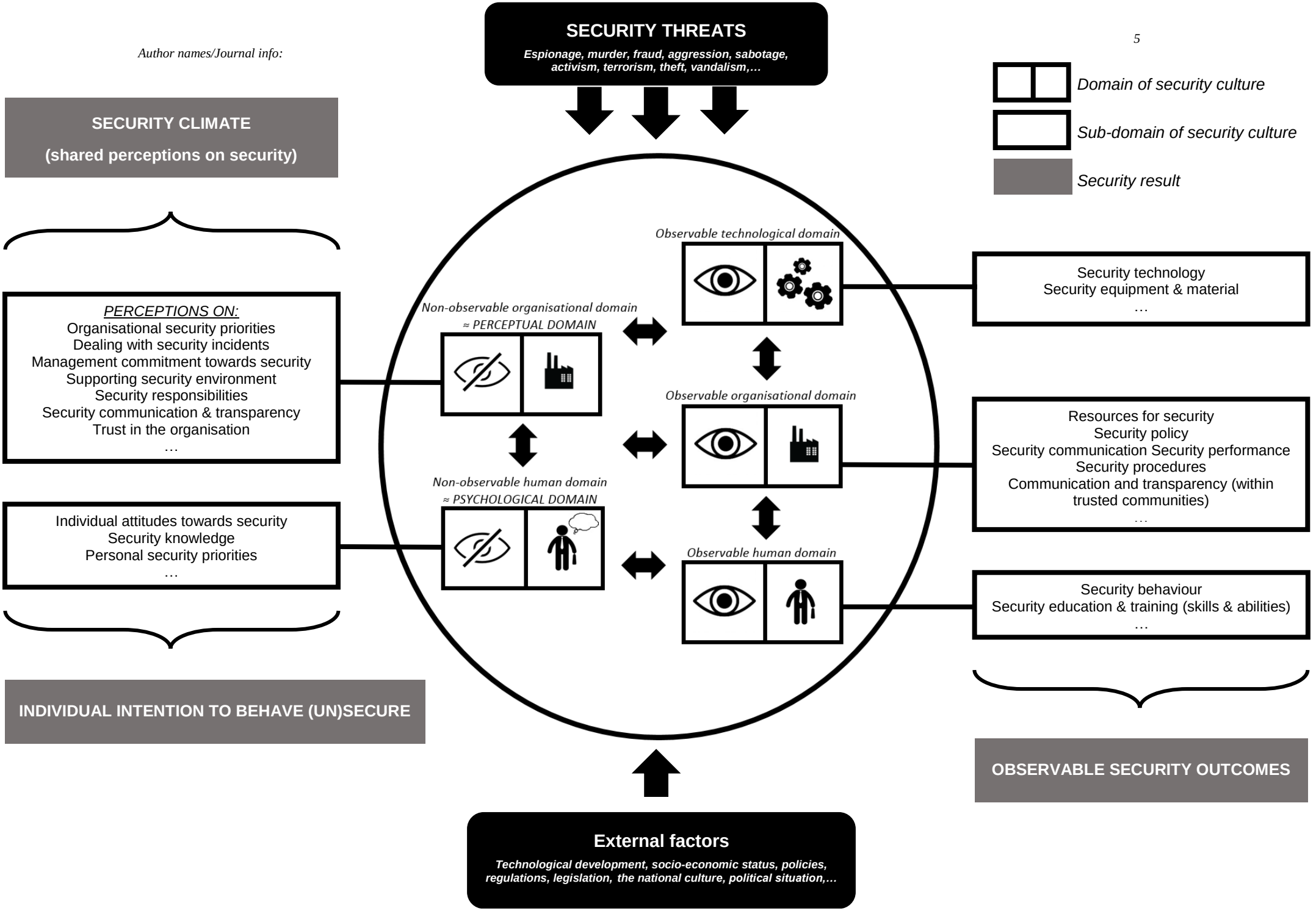

Fig. 1. An integrative conceptual framework for physical security culture in organisations

4. Addressing the security culture of an organisation

To address the physical security culture of an organisation, several steps should be taken as illustrated in Figure 2. Firstly, the security culture should be diagnosed. In order to obtain a clear image of the current physical security culture in the organisation, all sub-domains constituting physical security culture should be measured.

Subsequently, based on this measurement, recommendations should be formulated and implemented in order to improve the current physical security culture (van Nunen et al., 2016). It is important that continuous attention is being paid to the security of a company. Follow-up is needed in order to meet with possible changes within the company as well as external developments and trends in the field of security. It is an everlasting process, a cycle of evaluation and maintenance or change.

During this continuous process of addressing security culture, some aspects should be taken into account, in analogy with addressing safety culture (van Nunen et al., 2016). It is for instance important to use a multi-method approach in order to adequately explore and understand the security culture of an organisation. Also, the involvement of the entire organisation is important. Employees, supervisors, managers, contractors, clients, suppliers, etcetera; all should be taken into account when diagnosing the security culture. This comprehensive involvement is not only crucial during the diagnose of the security culture, but also during the phase of formulating improvement strategies and setting priorities. Not only leads this comprehensive involvement to a more accurate diagnose of the security culture, it also leads to the creation of a foundation to successfully implement and maintain the improvement strategies.

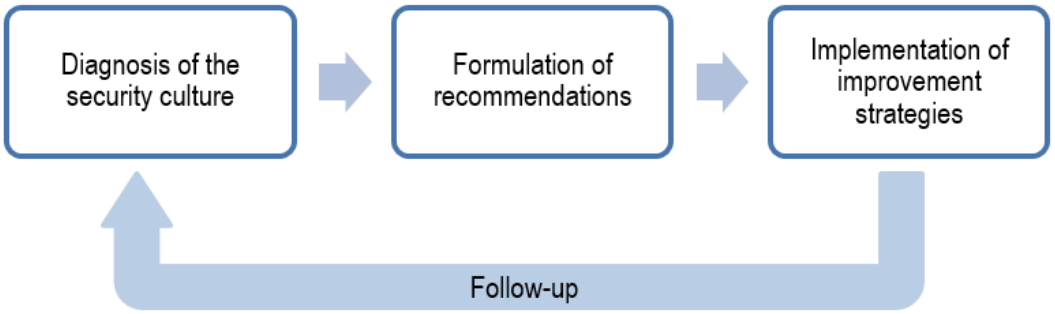

Fig. 2. Addressing physical security culture (adapted from van Nunen et al., 2016)

5. Conclusion

The proposed conceptual framework for physical security culture in organisations has the advantage that it brings technique, organisation and human together in a coherent, integrative and related way. The aim of the framework is to take all security-related aspects into account, leading to a pro-active approach of the physical security, instead of working on an incident-driven base. The framework provides specific points of departure to make the security culture measurable, and by extension controllable. The importance of continuous attention for security is being stressed, as well as the importance of the involvement of the entire organisation in order to obtain sustainable improvements in the field of security.

References

Connolly P.J. Security starts from within. InfoWorld, 2000; 22: 39-40.

Hopkins A. Studying organisational cultures and their effects on safety. Safety Science, 2006; 44: 875-889.

Jore S.H. The conceptual and scientific demarcation of security in contrast to safety. European Journal for Security Research. 2017; https://doi.org/10.1007/s41125-017-0021-9

Kria S, Pietre-Cambacedes L, Bouissou M, Halgand Y. A survey of approaches combining safety and security for industrial control systems. Reliability engineering & system safety, 2015; 139: 156-178.

Ruighaver A.B, Maynard S.B, Chang S. Organisational security culture: Extending the end-user perspective. Computers and Security, 2007; 26: 56-62.

van Nunen K, Reniers G, Ponnet K. Measuring and improving safety culture in organisations: an exploration of tools developed and used in Belgium. Journal of Risk Research. 2016; https://doi.org/10.1080/13669877.2016.1235602

Vierendeels G, Reniers G, van Nunen K, Ponnet K. An Integrative Conceptual Framework for Safety Culture: The Egg Aggregated Model (TEAM) of Safety Culture. Safety Science, 2018; 103: 323-339.