Cybersecurity Culture from the Perspective of Social Cognitive Theory: Examining the Relevance of the Reciprocal Determinism Model

Slađana Ćurčić

Introduction

With the development of sophisticated technologies and the digitization of society, cyber security has become an important issue at the national, societal, and individual levels. In other words, as a result of the growth and spreading of computer networks into whole aspects of life, cyber security is no longer a “special” and “extraordinary” issue but a kind of security much embedded into the everyday realities of people, states, and non-state actors (Cavelty, 2010a). While an increasing number of countries are adopting cyber security strategies, each individual must develop their own strategy to protect herself or himself against cybersecurity challenges in everyday

Slađana Ćurčić, Junior Research Assistant, Institute of European Studies, Belgrade
ORCID: 0000-0001-8276-0983, email: sladjana.curcic@ies.rs

DOI: https://doi.org/10.5281/zenodo.14204694

life. Cybersecurity culture is considered that kind of individual strategy. This is why this relatively recent concept in academic literature is gaining more and more prominence in practice and academic research. Its emergence induced academic curiosity about an adequate theoretical perspective for researching and explaining the concept. The reciprocal determinism model of security culture (RD model hereinafter), derived from Social Cognitive Theory (SCT), appears to be one of the potentially valuable frameworks. Its significance relies on the interdependence of three key factors: organizational, psychological, and behavioral, which capture the usual elements of security culture in general and, so, cyber security culture. This paper seeks to, through the systematization of the application of the RD model in cyber security culture research, indicate its importance and potential scope for a deeper understanding of this relatively new concept. At the same time, adequate theoretical framing and a clearer definition of the concept elements will contribute to the possibility of developing and improving cyber security culture on a practical level as well.

The improvement of cybersecurity culture becomes more and more important when we consider the potential cyber risks to which we are exposed on a daily basis, which most often come from the online sphere, which has become an integral part of our lives, whether through work, study, or entertainment. This also applies when it comes to the functioning of critical infrastructure, which is impossible without the Internet and a complex system of electronic communication connections (e.g., healthcare facilities, energy plants, banks, traffic infrastructure, etc.). In all these cybersecurity considerations, humans are the weakest link, as they could be potential targets of cyber attacks or even unknowingly participate in a cyber attack (Von Solms and Van Niekerk, 2013). Positioning this issue in the broader context of cyber security, it could be said that the common characteristic of different definitions of cybersecurity is that they try to be holistic and to include human aspects (The International Telecommunications Union (ITU), 2008; Von Solms and Van Niekerk, 2013; Schatz, Bashroush and Wall, 2017), which is actually the main difference between the notion of cyber security and information security. Speaking about these differences, it should be emphasized that cyber security goes beyond the boundaries of information security to include not only the protection of information resources but also that of other assets, including the person himself or herself (Von Solms and Van Niekerk, 2013).

This fact that the human factor is decisive for cyber security—people's behavior, awareness, knowledge, beliefs, and attitudes made socio-psychological theories often used in cyber security culture research and cyber security in general. For example, some researchers combined institutional theory and protection motivation theory in exploring security awareness through the lenses of cybersecurity culture (Andronache, 2021). Other authors explored the impact of protection motivation theory and general deterrence theory on active cyber defense (White, 2017). Technology threat avoidance theory (TTAT) is also a valuable framework for understanding individual threat avoidance motivation and behavior, which is a critical component in designing effective cybersecurity solutions for both users and organizations (Carpenter et al., 2019). So it is also used in researching the coping responses of employees to a cyberattack, especially concerning human and emotional aspects of cybersecurity (Stacey et al., 2021).

It can be concluded that a specific field such as cyber security very often requires the integration of theories closely related to cyber security and socio-psychological theories, which elucidate that very important human aspect. That's why many authors emphasize the need for an interdisciplinary approach in cybersecurity and cybersecurity culture research, combining information systems theories with social science theories like the Theory of Planned Behavior (TPB), Rational Choice Theory (RCT), Protection Motivation Theory (PMT), Theory of Reasoned Action (TRA), and Social-Cognitive Theory (SCT) (Hanna, 2020; Maalem Lahcen et al., 2020; Rohan et al., 2021; Ogden, 2021; Georgiadou et al., 2022). Those are, of course, valuable insights and recommendations for future research, but the state-of-the-art, as evidenced in the literature, shows that researchers usually study cybersecurity culture by assessing its level through surveys without relying on a concrete theoretical framework. For now, SCT, because of the compatibility of its RD model (a triad of factors: organizational (environmental), psychological (cognitive), and behavioral) with usual cybersecurity culture elements, appears to be the most adequate to fulfill this gap. From these insights arises the research question of the paper: What is the theoretical relevance of cybersecurity culture research through the RD model, and what are the potentials for practical improvement of cybersecurity culture by applying this model?

In order to answer the research question, first the theoretical basis in the subject field will be analyzed: academic thematization of cyber security, current knowledge, and scope of research on the concept of cybersecurity culture. Then, the basics of SCT and the RD will be presented, along with an overview of their applications in security culture research. Based on the summarization of the literature review and content analysis of existing cybersecurity culture models, the central part of the paper will provide an overview of the cybersecurity culture models based on reciprocal determinism.

Cyber Security: Theoretical Considerations

Social, political, and technological developments that transform our daily lives but also shape the reality of security are, at the same time, key factors in the growing importance of the field of cyber security. Following the introduction of personal computers in the 1980s, when the term cyber-crime was born with the development of cyber-counterculture," and then the 1980s and 1990s, when the debate on cyber threats was influenced by the post-Cold War strategic context, it is clear that cyber security actually evolved in line with the information revolution (Cavelty, 2010a). Today, as a result of the growth and spreading of computer networks into whole aspects of life, cyber security is no longer a "special" and "extraordinary" issue but a kind of security much embedded into the everyday routines of people, states, and non-state actors (Cavelty, 2010a).

Speaking specifically about the definition of the term cyber security, many authors tried to provide a more complete and clearer definition by realizing the shortcomings of the existing definitions. Some of them find that the term is used broadly and that its definitions are highly variable, context-bound, often subjective, and, at times, uninformative (Craigen, Diakun-Thibault, and Purse, 2014). They argue that the absence of a definition that captures the multidimensionality and interdisciplinarity of cybersecurity potentially impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity (Craigen, Diakun-Thibault, and Purse). So, they provided, as they say, an inclusive, meaningful, and unifying definition that could fill this theoretical gap: “Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights” (Craigen, Diakun-Thibault, and Purse, p. 17). Others claim that the goal of cyber security is to secure those that function in cyberspace, whether individuals, organizations, critical national infrastructure, societies, or nations. Relying on that position, they define cyber security “as the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal, and national capacities, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace” (Von Solms and Van Niekerk, 2013, p. 101).

A group of authors also conducted an interesting review and content analysis of cyber security definitions classified into three main categories: industry definitions, government and nation-state definitions, and academic definitions, and as a result, they created a new definition comprising the key terms identified (Schatz, Bashroush, and Wall, 2017). According to them, “cyber security refers to the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity, and availability of data and assets used in cyber space. The concept includes guidelines, policies, and collections of safeguards, technologies, tools, and training to provide the best protection for the state of the cyber environment and its users” (Schatz, Bashroush, and Wall, 2017, p. 66). In addition to the academic definitions, it should also be mentioned the approach that the International Telecommunications Union (ITU) advocates. It defines cyber security as “a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment, organization, and user's assets" (ITU, 2008, p.). It could be said that the common characteristic of the above definitions is that they try to be holistic and to include human aspects, which is actually the main difference between the notions of cyber security and information security.

Regarding these differences, it should be emphasized that cyber security goes beyond the boundaries of information security to include not only the protection of information resources but also that of other assets, including the person himself or herself. So, in cyber security, humans are considered potential targets of cyber attacks or even unknowingly participating in a cyber attack, while in information security, reference to the human factor usually relates to the role(s) of humans in the security process (Von Solms and Van Niekerk, 2013). But what is common both to information and cyber security measures is the goal of ensuring confidentiality, integrity, and availability of information (Stoneburner, 2001; ITU, 2008). Briefly, it should also be said that the three main types of cyber threats are cybercrime, cyberterrorism, and cyberwar (Cavelty, 2010b), but cyberbullying could also be added (Kaur and Ramkumar, 2022). Then, regarding cybercrime, according to the UK's Crown Prosecution Service (CPS), there are two broad categories: cyber-dependent (e.g., hacking, malware, denial of service) and cyber-enabled crimes (financial fraud, phishing, pharming, extortion) (CPS, 2019).

The Concept of Cybersecurity Culture

Academic literature, but also the everyday reality we live in, shows that changes and development of the concept of security culture are conditioned by changes in security reality. Transformations in the understanding and manifestations of security culture, especially happen when they are necessary for serious social adjustments (Buluc, Lungu, and Deac, 2018), In this sense, the Chernobyl nuclear disaster, the terrorist attack on the USA in 2001, the development of information technologies, but also pandemics of infectious diseases, are events and processes that represent important milestones in the development of security culture, both as a concept and as a practice. So, the still-increasing development of information and the cyber sphere refers to the security field, in which cyber security culture has gained great importance.

As it was previously elaborated that cyber security is a broader concept than information security, the same can be said for the relationship between cyber and information security cultures. Also, it should be said that the concept of information security culture has been studied for a significantly longer period (Uchendu et al., 2021) and is more established (Reid and Van Niekerk, 2014). Therefore, it is understandable that there is much more knowledge about information security culture, which is sometimes uncritically applied to cyber security culture. But what is the common acknowledgment of many authors in the elucidation of these differences and overlappings is the emphasizing of the human factor as indispensable while studying cyber security culture (Gcaza et al., 2017; Georgiadou et al., 2022; Mwim and

Mtsweni, 2022). An additional explanation of the differences is that information security culture emphasizes behaviors that comply with information security policy, but a cybersecurity culture includes not only compliance with policy but also personal involvement in organizational cyber safety (Huang and Pearlson, 2019). In order to give more clarity, these authors offer a definition of organizational cybersecurity culture, which means "the beliefs, values, and attitudes that drive employee behaviors to protect and defend the organization from cyber attacks" (Huang and Pearlson, 2019, p. 6399). However, some authors still think that cybersecurity culture is an ill-defined problem, especially because of the lack of clarity in the academic community about the definition of cybersecurity culture, the lack of research focusing on measuring cybersecurity culture, and consequently, the absence of a solution for cultivating cybersecurity culture (Gcaza and Solms, 2017). Regardless, what is indisputable is that cybersecurity culture is necessary for encouraging acceptable user behavior in the reality of cyberspace (ITU, 2008). Additionally, other authors think that the process of raising a cyber security culture could function as a self-learning process for organizations by producing valuable insights regarding organizational values, norms, etc. (Karyida, 2017).

In the understanding of cyber security culture, some authors adhere to Schein's model of organizational culture and argue that cyber security culture consists of several layers: artifacts, espoused values, tacit assumptions, and their respective contents (Reegrd, Blackett, and Katta, 2019). Actually, these authors are speaking about organizational cyber security culture (according to their understanding of cybersecurity culture as a sub-component of organizational culture), but they remind us that cybersecurity extends beyond the organizational boundaries, and therefore, research on the influence of factors external to the organization on cybersecurity culture is needed. Further, they state that key practices for developing cybersecurity culture resemble those highlighted in the literature on safety culture: management support, policy, awareness and training, involvement and communication, and learning from experience (Reegrd, Blackett, and Katta, 2019). Other authors also follow this line of thinking, relying on Schein's model (and adding knowledge as a fourth level) in defining firstly information security culture and then arguing that cyber security culture consists of the same components but with a bit of different content due to the different contexts in which the cultures foster (Reid and Van Niekerk, 2014). More specifically, information security culture is cultivated and managed within insulated organizational contexts, which are relatively well controlled environments with relatively predictable user behavior, activity, and profile sets. On the other side, cyber-security culture would be cultivated within a societal environment that would likely be less controlled (Reid and Van Niekerk, 2014).

A comprehensive model of cyber security culture entails two levels: organizational and individual, divided into different dimensions. The organizational level is divided into the following dimensions: assets, continuity, access, and trust; operations; defense; and security governance. Individual dimensions are attitude, awareness, behavior, and competency. Each dimension consists of domains with distinctive application areas and quantifiable indicators (Georgiadou et al., 2020). For Da Veiga (2016), cybersecurity culture should ideally be fostered at all levels, including individual, organizational, national, and international levels. In this context, it is an interesting attempt to define cybersecurity culture from the perspective of strategic culture (Tziarras, 2014). Actually, this author starts from the broader framework of the changing concept of security and focuses on cultivating cybersecurity culture on a global level through multi-leveled collaboration. So, he defines a security culture of multileveled cybersecurity "as a body of collective (non-state, sub-national, and national) attitudes, patterns of behavior, and beliefs, as well as conceptions of (cyber) security, shaped based on the need to secure multiple referent objects against various cyber threats, which would influence cybersecurity strategies" (Tziarras, 2014, p. 330). Regarding the previous criticism about the lack of methodological solutions in measuring cyber security culture, the meta-analysis of cyber security culture research shows that not all studies aim to provide a method in which security culture can be measured or assessed but to present a framework or approach in which a security culture can be built and maintained (Uchendu et al., 2021). Moreover, this analysis found that questionnaires, surveys, and interviews are widely used in measuring the level of cyber security culture (Uchendu et al., 2021). Of course, as Uchendu and colleagues emphasize, any proposal of a framework at a conceptual or theoretical level should be carefully considered regarding the possibility of assessment in practice. So, they add that there is a need for testing and evaluation of proposed security culture approaches and frameworks to provide real-world evidence of their efficacy (Uchendu et al., 2021).

Finally, it can be said that the operationalization of cybersecurity culture also depends on the specific perspective of researchers and contexts of application, but as previous analysis has shown, most authors agree on some key elements of the concept. Certainly, the integration and communication of different disciplines will potentially contribute to a better and more precise determination of the concept.

Reciprocal Determinism Model of Safety Culture[1]

The reciprocal determinism model originates from Albert Bandura's Social Cognitive Theory (SCT), which subscribes to a model of emergent interactive agency (1986). Bandura describes *triadic reciprocal causation* or *triadic reciprocal determinism* as a model in which "action, cognitive, affective, and other personal factors, and environmental events all operate as interacting determinants" (1989, p. 1175). Respectively, he explains it by the fact that persons are neither autonomous agents nor simply mechanical conveyers of animating environmental influences. Rather, they make a causal contribution to their own motivation and action within a system of triadic reciprocal causation (1989, p. 1175). Even though these factors operate as interacting determinants that influence each other bidirectionally, Bandura empathizes that it doesn't mean that the different sources of influence are of equal strength, nor do the reciprocal influences all occur simultaneously. Actually, some influences may be stronger

[1] In his research on reciprocal determinism, Cooper used the term *safety culture*, so original term was kept, but when reffering to the cyber context, it will be used the term *security culture.* Namely, as a key difference between the concepts of safety and security, and thus safety and security culture, the literature emphasizes the origin of undesirable events, which are unintentional in the field of safety (incidents, natural disasters), and intentional in the field of security (actions that are designed and planned to cause harm, e.g. terorrist attacks, cyber threats) (Stanarević, 2012; Mattila, 2013; Sas et al., 2021). However, the greatest similarity is that both safety and security are part of the overall culture of the organization (Sas et al., 2021).

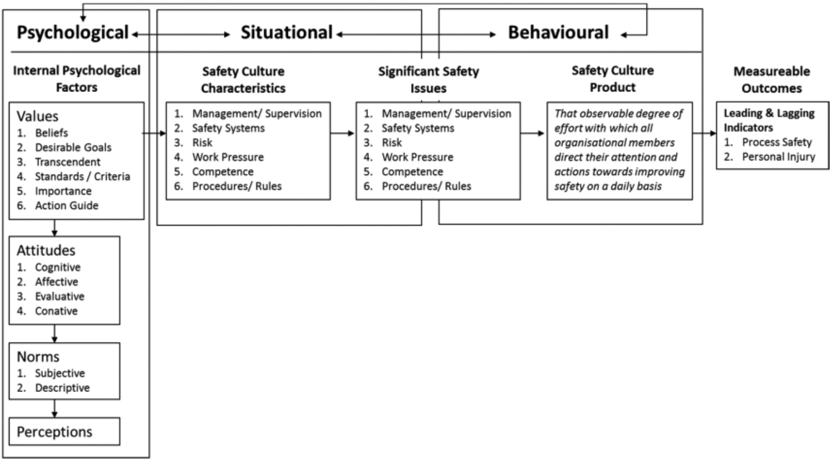
than others, and it takes time for a causal factor to exert its influence and activate reciprocal influences (Bandura, 1999). In other words, this bidirectionality of influence means that “people are both products and producers of their environment” (Wood and Bandura, 1989, p. 362).

This interdependence of behavioral, psychological, and social factors was found to be insightful by some authors as a theoretical and practical framework to measure and analyze safety culture. Thus, Bandura’s model of reciprocal determinism was adapted by Cooper (1994, 1997a, b, 2000, 2002, 2016, 2018), to research safety culture, resulting in what is called the reciprocal determinism model of safety culture. It contains three elements, which encompass subjective internal psychological factors, observable ongoing safety-related behaviors, and objective situational features (Cooper, 2000). As can be concluded from the Picture 1, Cooper defines safety culture as “the product of multiple goal-directed interactions between people (psychological), jobs (behavioral), and organizations (situational)”[2] and actually sees it as dynamic reciprocal relationships between those elements (Cooper, 2002, p. 32). So, this is exactly where the compatibility between the

[2] Originally, Cooper’s reciprocal safety culture model implied this sequence: psychological aspects—behavioral aspects—situational aspects (Cooper, 2000). Later, as can be seen from the attached picture, the revised model implied behavior at the end. This resulted from his insight that changes in certain procedures and rules (organizational factors) will affect behavior change, which will then increase safety performance and reduce incidents (which will in turn positively affect psychological factors), rather than the changes in core basic assumptions and attitudes (psychological factors) will lead to a behavior change (Cooper, 2016).
In his words ”The principle is to optimise the situation to optimise the behaviour. In turn, as the desired behaviours become habitual, the various psychological factors will become more positive” (Cooper, 2018, p. 51).

reciprocal determinism model and the nature of safety culture lies. Additionally, the potency of the RD model for analyzing safety culture, according to Cooper, also lies in the fact that it provides a triangulation methodology that allows researchers to holistically examine safety culture as a complex, multi-faceted construct. Thus, the reciprocal relationships between psychological, behavioral, and situational factors can be examined with a view to establishing antecedents, behaviors, and consequences within specific contexts (Cooper, 2000). Specifically, speaking about measurement, he emphasizes that internal psychological factors (i.e., attitudes and perceptions) are assessed via safety climate questionnaires, safety-related behavior is assessed via checklists developed as a part of behavioral safety initiatives, and situational features are assessed via safety management system audits and inspections (Cooper, 2000).

Picture 1: *Cooper's reciprocal safety culture model (2016).*



Since the core of the safety culture construct is about "proactively managing safety, thinking positively about safety, and behaving safely" (Cooper, 2016, p. 4), deepening the theoretical basis of the concept and ways of its practical improvement is gaining more and more importance. Many authors recognized the potential of Cooper's RD model of safety culture and applied it to safety culture research in various contexts, mostly in high-risk industries. Based on Cooper's safety culture model, Choudhry, Fang, and Mohamed (2007a) have developed a conceptual model of construction safety culture. The model is anchored in three fundamental conceptual categories, namely, safety climate, behavior-based safety, and safety system. The model offers an integrative framework and can be applied to construction projects to maintain and improve construction site safety. It reveals that unsafe conditions can be traced through the site safety implementation and can be rectified (Choudhry, Fang, and Mohamed, 2007b). Consequently, it appeared that Cooper's model could really be fruitfully applied in the construction industry, so other authors also applied it, trying to even revise and improve the previously offered model by Choudhry, Fang, and Mohamed (Ismail et al., 2009; Alasamri, Chrisp, and Bowles, 2012).

Based upon a modified version of Cooper's reciprocal determinism model, the study on safety culture in the fire service uses two sets of exogenous variables, labeled Safety Management System and Safety Related Behaviors, to explain a dependent variable called Organizational Safety Climate (Pessemier and England, 2012). Some authors researched safety behaviors among firefighters and the safety culture of the department, relying on SCT and reciprocal determinism but without special reference to Cooper's model of safety culture (Freaney, 2011). Of course, there are authors who didn't explicitly use Cooper's model of safety culture but implicitly supported it and indicated its relevance by studying behavioral, organizational, and psychological elements of safety culture in their studies, predominantly related to the Occupational Health and Safety (OHS) domain (Fernandez Muniz et al., 2007; Lefranc et al., 2012).

In addition to the evident academic curiosity about the RD model of safety culture, its practical relevance is also reflected in the fact that this exact approach has been officially adopted as a standard by the American Petroleum Institute and the American National Standards Institute (Cooper, 2018). Additionally, while comparing other safety culture models and finding similarities and differences with the RD model, Cooper pointed out that it would appear that the reciprocal model has some general applicability, particularly as it incorporates the underlying features of existing safety culture models and allows both the qualitative and quantitative aspects of safety culture to be explored (Cooper, 2000). Moreover, as he noted, the RD model of safety culture encompasses some models, like the "Total Safety Culture' model. So, he concludes that the RD model of safety culture has the potential to facilitate future meta-analyses of safety culture research (Cooper, 2000).

Research Findings: Application of the Reciprocal Determinism Model in Cybersecurity Culture Research

Table 1 represents the results of the literature review, which aimed to find cybersecurity culture models based on the social cognitive framework, specifically the RD model of security culture. Analysis revealed that there is no cybersecurity culture model directly based on the RD model, but there are several cybersecurity culture models that could be labeled as partially consistent with the RD model. This conclusion is derived from the essence of the presented cybersecurity culture models. Specifically, elements of these models are reorganized according to three key aspects of the RD model. Of course, these models do not exhaust all the elements contained in the RD model, and they differ in their terms and meanings, which is expected as a reflection of the specificity of the field of cyber security. What is important is that the elements of the listed cyber security culture models, according to the logic of their meaning, can be classified as psychological, organizational, or behavioral factors. This also means that all authors (implicitly or explicitly through the models used) recognize that cybersecurity culture necessarily implies the interaction of these three levels. Also, as could be noted, a group of almost the same authors explored the same model of cybersecurity culture in different sectors: healthcare systems, remote working, critical infrastructure, as well as the energy sector. This is also important in an effort to empirically test the model and determine its applicability in different contexts.

These results could be considered as a part of the evidence about the relevance of the RD model in cybersecurity culture research. The general use of Social Cognitive Theory in cybersecurity culture research also gives indirect and valuable insights about the potency of the RD model. For example, SCT has been used to study individuals' responses to specific cyber security threats, like phishing. Specifically, SCT was used to examine the influence of the triadic factors of perceived self-efficacy toward antiphishing behaviors, expected negative

Table 1: *Cybersecurity culture models based on the reciprocal determinism model.*

Authors	Cybersecurity culture model	Industry/field	Consistent with RD model of security culture
Huang and Pearlson (2019)	**External influences** Societal cybersecurity culture External rules and regulations Peer institutions **Organizational mechanisms** Cybersecurity culture leadership Performance evaluations Rewards and punishments Organizational learning Cybersecurity training Communications channel **Beliefs** **Attitudes** **Values** (at leadership, group and individual level) **Behaviors** In-role cybersecurity behavior Extra-role cybersecurity behavior	**Organizational context**	**Partially** **Psychological aspect** Beliefs Attitudes Values **Situational** External influences Organizational mechanisms **Behavioral** In-role cybersecurity behavior Extra-role cybersecurity behavior

Authors	**Cybersecurity culture model**	**Industry/field**	**Consistent with RD model of security culture**
Kabanda and Chingoriwo (2021)	**Five pillars:** Shared national cybersecurity vision and strategy ICTs and related infrastructure Cybersecurity legislation Education and awareness Technology framework and skills	**General**	**Partially** **Psychological aspect** Awareness **Situational** Shared national cybersecurity vision and strategy ICTs and related infrastructure Cybersecurity legislation Technology framework **Behavioral** Education Skills
Georgiadou, Mouzakitis and Askounis (2021)	**Organizational level** Assets Continuity Access and trust Operations Security governance Defense **Individual level** Attitude Competency Behavior Awareness	**General**	**Partially** **Psychological aspect** Attitude Awareness **Situational** Assets Continuity Access and trust Operations Security governance Defense **Behavioral** Competency Behavior
Georgiadou, Mouzakitis and Askounis (2021)		**Crictical infrastructure**	
Gioulekas et al. (2022)		**Healthcare**	
Georgiadou, Michalitsi-Psarrou and Askounis (2022)		**Energy sector**	
Georgiadou, Mouzakitis and Askounis (2022)		**Remote working**	

outcomes from reporting spear phishing emails, and cybersecurity self-monitoring on individuals' likelihood of reporting spear phishing emails. By adding the construct of cyber risk beliefs (CRBs) into the SCT framework, the research model explained the motivational factors that inhibit the reporting of spear phishing (Kwak et al., 2020). In a similar way, Ogden (2021) used Social Cognitive Theory to identify factors that influence human security behavior and best practices for developing a cybersecurity culture while focusing on the relationships between 1) environmental factors, 2) cognitive factors (personal factors), and 3) their mediating effects on behaviors. Research has shown that social proximity, subjective norms, descriptive norms (environmental factors), self-efficacy, knowledge, and experience (cognitive factors) are contributing factors that influence an individual to perform cyber-secure behaviors (Ogden, 2021).

Additionally, SCT is successfully used in exploring cybersecurity awareness, which is closely related to cybersecurity culture (Hanna, 2020). Components of SCT were demonstrated to be important concepts for promoting and fostering desired cybersecurity behavior in organizations across industry domains. Specifically, by assuming that employees are agents and their behavior and learning are directed by the triadic reciprocal determinism model, organizational IT leaders can incorporate adequate SETA strategies (security education, training, and awareness) and foster environments that promote cybersecurity behavior and improve cybersecurity culture. Consequently, improved cybersecurity culture and learned cybersecurity practices could also be applied in the home context (Hanna, 2020).

From the points above, the authors' efforts in searching for the most adequate framework for cybersecurity culture are evident. Moreover, almost all the analyzed research involved empirical validation of the specific cybersecurity culture model. In this sense, connecting theoretical knowledge with practical solutions for the development and improvement of cyber security culture will undoubtedly contribute to this field. Generally speaking, experts in this field always remind us that collaboration and constant communication between researchers, practitioners, academia, and industry are of great importance for improving the body of knowledge on cybersecurity culture and security culture in general (Uchendu et al., 2021; Cooper, 2016).

Conclusion

It is obvious that the application of the RD model in the study of cyber security culture has not yet caught on, as is the case with security culture in general. However, systematization of the existing cybersecurity culture models revealed that the most common elements that predominantly determine cybersecurity culture are organizational and individual (which include behavioral in some cases). From a practical point of view, this should remind us of the role of humans and human factors in the cybersphere as an emerging part of our everyday lives. So, the current research could be relevant both for organizations and individuals by emphasizing that developing and improving the cybersecurity culture is the best strategy to ensure cyber security in such a fragile digital world, which faces us with threats at work, at home, at school, etc.

Addressing the research question, the potency of the RD model in cybersecurity culture research is recognized in the presence of three broader aspects (psychological, organizational, and behavioral) of security culture in all selected models, with varying elements. Moreover, this diversity of elements of cybersecurity culture actually speaks about the complexity of the concept and can help researchers consider what levels and elements should be taken into account in order to study and understand cybersecurity culture in depth.

Relevance of the RD model is also evident in the application of SCT in a broader cybersecurity context. This lies in the fact that SCT is the well-established, validated, and mostly used theory on behavior change, while on the other hand, understanding the human factor, i.e., human behavior and its constant interaction with the environment, is becoming increasingly important for cybersecurity culture research and practice. Thus, offering adequate theoretical framing of the cybersecurity concept, which is a precondition for its assessment and practical improvement, is what makes the RD model and, broader, SCT, worth the attention of researchers in the study of cybersecurity culture.

Morever, engaging theoretical frameworks from psychology, sociology, and organizational behavior in cybersecurity culture research is in favor of interdisciplinarity in the research and is valuable for "both sides". Namely, in such a way, these theories could be tested in a specific context and thus improve their value, while at the same time providing insight into broader aspects of cybersecurity cuThe relevanceat are not covered by "more traditional" theories in this field (e.g., information systems theories).

Besides useful insights from this research, it should be said that the main limitation lies in the fact that all selected models are partially consistent with the RD model (based on the author's reorganization of the elements according to three key aspects). The main reason for this could be seen in the state-of-the-art: the concept of cybersecurity culture is relatively recent and does not have a long history of study. Although cybersecurity is a growing field, it is not surprising that no model directly based on the RD model has been found, as researchers are still exploring the field and searching for the most adequate theoretical underpinning and conceptual framework for cybersecurity culture. So, all findings and conclusions from this paper could serve as an impetus for the future wider application of the RD model in cybersecurity culture research. One of the recommendations to the researchers refers to the testing of existing models of cybersecurity culture based on the RD model in order to empirically verify and revise them and thus come to new knowledge, which would be integrated back into the theory. Of course, more replicative studies of cybersecurity culture, based both on SCT and other theories, from a broader perspective will contribute to finding the most suitable model of cybersecurity culture.

References

Andronache, A. (2021). Increasing security awareness through lenses of cybersecurity culture. *Journal of Information Systems and Operations Management, 15*(1), 7–22.

Alasamri, H., Chrisp, M. T., & Bowles, G. (2012). A framework for enhancing and improving the safety culture on Saudi construction sites. In S. D. Smith (Ed.), *Proceedings of the 28th Annual ARCOM Conference* (pp. 475-485). Association of Researchers in Construction Management. https://www.arcom.ac.uk/-docs/proceedings/ar2012-0475-0485_Alasamri_Chrisp_Bowles.pdf

Bandura, A. (1986). *Social foundations of thought and action: A social-cognitive view.* Prentice Hall.

Bandura, A. (1989). Human agency in social cognitive theory. *American Psychologist, 44*(9), 1175–1184. https://doi.org/10.1037/0003-066X.44.9.1175

Bandura, A. (1999). Social cognitive theory: An agentic perspective. *Asian Journal of Social Psychology, 2*(1), 21–41. https://doi.org/10.1111/1467-839X.00024

Bandura, A., & Wood, R. E. (1989). Effect of perceived controllability and performance standards on self-regulation of complex decision-making. *Journal of Personality and Social Psychology, 56*(5), 805–814. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=a5989e-20385c9972919084a9ed357b103625aeb9

Buluc, R., Lungu, C., & Deac, I. (2018). Perceptions on security culture. *Redefining Community in Intercultural Context, 7*(1), 149–156. https://www.ceeol.com/search/article-detail?id=874195

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems, 44*, 380–407. https://doi.org/10.17705/1CAIS.04422

Cavelty, M. D. (2010a). Cyber-security. In P. J. Burgess (Ed.), *The Routledge Handbook of New Security Studies* (pp. 155-162). Routledge. https://doi.org/10.4324/9780203859483

Cavelty, M. D. (2010b). Cyber-threats. In M. D. Cavelty & V. Mauer (Eds.), *The Routledge Handbook of Security Studies* (pp. 180-189). Routledge.

Choudhry, R. M., Fang, D., & Mohamed, S. (2007a). Developing a model of construction safety culture. *Journal of Management in Engineering, 23*(4), 207-212. https://doi.org/10.1061/(ASCE)0742-597X(2007)23:4(207)

Choudhry, R. M., Fang, D., & Mohamed, S. (2007b). The nature of safety culture: A survey of the state-of-the-art. *Safety Science, 45*(10), 993–1012. https://doi.org/10.1016/j.ssci.2006.09.003

Cooper, M. D. (1994). Implementing the behaviour-based approach to safety: A practical guide. *The Health and Safety Practitioner, 12*(11), 18–23. http://behavioural-safety.com/articles/Implementing_Behavior_Based_Safety_a_practical_guide.pdf

Cooper, M. D. (1997a). Evidence from safety culture that risk perception is culturally determined. *The International Journal of Project and Business Risk Management, 1*(2), 185–202.

Cooper, M. D. (1997b). *Improving safety culture: A practical guide.* J. Wiley.

Cooper, M. D. (2000). Towards a model of safety culture. *Safety Science, 36*(2), 111–136. https://www.behavioral-safety.com/articles/Towards_a_model_of_safety_culture.pdf

Cooper, M. D. (2002). Understanding and quantifying safety culture: A reciprocal model for success. *Professional Safety, 47*(6), 30–36.

Cooper, M. D. (2016). *Navigating the safety culture construct: A review of the evidence.* B-Safe Management Solutions Inc. https://www.behavioral-safety.com/articles/safety_culture_review.pdf

Cooper, M. D. (2018). The safety culture construct: Theory and practice. In C. Gilbert, B. Journé, H. Laroche, & C. Bieder (Eds.), *Safety cultures, safety models: Taking stock and moving forward* (pp. 47-61). Springer. https://doi.org/10.1007/978-3-319-95129-4_5

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13-21. https://www.timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf

Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In *2016 SAI Computing Conference (SAI)* (pp. 1006-1015). IEEE. https://doi.org/10.1109/SAI.2016.7556102

Fernández-Muñiz, B., Montes-Peón, J. M., & Vázquez-Ordás, C. J. (2007). Safety culture: Analysis of the causal relationships between its key dimensions. *Journal of Safety Research, 38*(6), 627–641. https://doi.org/10.1016/j.jsr.2007.09.001

Freaney, C. (2011). *Safety culture and safety behaviors among firefighters* [Doctoral dissertation, University of Tennessee]. TRACE. https://trace.tennessee.edu/utk_graddiss/969

Gcaza, N., & von Solms, R. (2017). Cybersecurity culture: An ill-defined problem. In M. Bishop, L. Futcher, N. Miloslavskaya, & M. Theocharidou (Eds.), *Information security education for a global digital society: WISE 2017* (pp. 98-109). Springer. https://doi.org/10.1007/978-3-319-58553-6_9

Gcaza, N., von Solms, R., Grobler, M. M., & Van Vuuren, J. J. (2017). A general morphological analysis: Delineating a cybersecurity culture. *Information and Computer Security, 25*(3), 259–278. https://doi.org/10.1108/ICS-12-2015-00

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK risk using a cybersecurity culture framework. *Sensors, 21*(9), 1–14. https://doi.org/10.3390/s21093267

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Designing a cybersecurity culture assessment survey targeting critical infrastructures during the COVID-19 crisis. *International Journal of Network Security and Its Applications (IJNSA), 13*(1), 33–50. https://doi.org/10.5121/ijnsa.2021.13103

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cybersecurity culture framework for assessing organization readiness. *Journal of Computer Information Systems, 62*(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

Georgiadou, A., Michalitsi-Psarrou, A., & Askounis, D. (2022). Evaluating the cybersecurity culture of the EPES sector: Applying a cybersecurity culture framework to assess the EPES sector's resilience and readiness. In *Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES'22)* (pp. 1–10). Association for Computing Machinery. https://doi.org/10.1145/3538969.3543813

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Working from home during the COVID-19 crisis: A cybersecurity culture assessment survey. *Security Journal, 35*(2), 486–505. https://doi.org/10.1057/s41284-021-00286-2

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y., Marin, S., Cabecinha, R., & Ntanos, C. (2022). A cybersecurity culture survey targeting healthcare critical infrastructures. *Healthcare, 10*(2), 1–19. https://doi.org/10.3390/healthcare10020327

Hanna, M. M. (2020). *Exploring cybersecurity awareness and training strategies to protect information systems and data* [Doctoral dissertation, Walden University]. ProQuest Dissertations and Theses Global.

Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. In T. X. Bui (Ed.), *Proceedings of the 52nd Hawaii International Conference on System Sciences* (pp. 6398-6407). University of Hawaii at Manoa. http://hdl.handle.net/10125/60074

International Telecommunications Union (ITU). (2008). *Series X: Data networks, open system communications and security: Telecommunication security. Overview of cybersecurity.* ITU.

Ismail, F., Hashim, A. E., Ismail, R., & Majid, M. Z. A. (2009). The operationalisation of safety culture for Malaysian construction organizations. *International Journal of Business and Management, 4*(9), 226–237. https://pdfs.semanticscholar.org/ae77/4ae366497a05d1c6efe187f1686263f7cb63.pdf

Kabanda, G., & Chingoriwo, T. (2021). A cybersecurity culture framework for grassroots levels in Zimbabwe. *Oriental Journal of Computer Science and Technology, 14*(1–3), 17–34. https://doi.org/10.13005/ojcst14.010203.03

Karyda, M. (2017). Fostering information security culture in organizations: A research agenda. In *The 11th Mediterranean Conference on Information Systems (MCIS) Proceedings* (pp. 1–11). Association for Information Systems. https://aisel.aisnet.org/mcis2017/28

Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cybersecurity: A review. *Journal of King Saud University-Computer and Information Sciences, 34*(8), 5766–5781. https://doi.org/10.1016/j.jksuci.2021.01.018

Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear phishing emails? *Telematics and Informatics, 48*(3), 101343. https://doi.org/10.1016/j.tele.2020.101343

Lefranc, G., Guarnieri, F., Rallo, J. M., Garbolino, E., & Textoris, R. (2012). Does the management of regulatory compliance and occupational risk have an impact on safety culture? In *11th International Probabilistic Safety Assessment and Management Conference and Annual European Safety and Reliability Conference (PSAM11 and ESREL 2012)* (pp. 6514-6523). IAPSAM and ESRA. https://hal-mines-paristech.archives-ouvertes.fr/hal-00734322

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity, 3*(1), 1-18. https://doi.org/10.1186/s42400-020-00050-w

Mattila, M. (2013). Different views on defining safety, security, and social responsibility. *Interdisciplinary Studies Journal, 3*(1), 7-20.

Mwim, E. N., & Mtsweni, J. (2022). Systematic review of factors that influence the cybersecurity culture. In N. Clarke & S. Furnell (Eds.), *International symposium on human aspects of information security and assurance* (pp. 147-172). Springer. https://doi.org/10.1007/978-3-031-12172-2_12

Ogden, S. E. (2021). *Cybersecurity: Creating a cybersecurity culture* [Doctoral dissertation, California State University]. Electronic Theses, Projects, and Dissertations. https://scholarworks.lib.csusb.edu/etd/1284

Pessemier, W. L., & England, R. E. (2012). Safety culture in the US fire service: An empirical definition. *International Journal of Emergency Services, 1*(1), 10–28. https://doi.org/10.1108/20470891211239290

Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. In M. Beer & E. Zio (Eds.), *29th European safety and reliability conference* (pp. 4036-4043). Research Publishing. https://doi.org/10.3850/978-981-11-2724-3_0761-cd

Reid, R., & Van Niekerk, J. (2014). From information security to cybersecurity cultures. In H. S. Venter, M. Laack, M. Coetzee, & M. M. Eloff (Eds.), *2014 Information security for South Africa* (pp. 1-7). IEEE. https://doi.org/10.1109/ISSA.2014.6950480

Rohan, R., Funilkul, S., Pal, D., & Chutimaskul, W. (2021). Understanding human factors in cybersecurity: A systematic literature review. In S. Paul & J. K. Verma (Eds.), *2021 International Conference on Computational Performance Evaluation* (pp. 133-140). IEEE. https://doi.org/10.1109/ComPE53109.2021.9752358

Sas, M., Hardyns, W., Van Nunen, K., Reniers, G., & Ponnet, K. (2021). Measuring the security culture in organizations: A systematic overview of existing tools. *Security Journal, 34*(2), 340–357. https://doi.org/10.1057/s41284-020-00228-4

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cybersecurity. *Journal of Digital Forensics, Security and Law, 12*(2), 53–74. https://doi.org/10.15394/jdfsl.2017.1476

Stacey, P., Taylor, R., Olowosule, O., & Spanaki, K. (2021). Emotional reactions and coping responses of employees to a cyber-attack: A case study. *International Journal of Information Management, 58*(3), 102298. https://doi.org/10.1016/j.ijinfomgt.2020.102298

Stanarević, S. (2012). *Koncept bezbednosne kulture i pretpostavke njegovog razvoja* [Doctoral dissertation, University of Belgrade]. https://fb.bg.ac.rs/download/RepozitorijumDisertacija/2012-11-09%20Stanarevic%20Svetlana/Disertacija.pdf

Stoneburner, G. (2001). *Computer security: Underlying technical models for information technology security*. National Institute of Standards and Technology (NIST). https://www.nist.gov/publications/underlying-technical-models-information-technology-security

The Crown Prosecution Service (CPS). (2019). *Cybercrime - prosecution guidance.* https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

Tziarras, Z. (2014). The security culture of a global and multileveled cybersecurity. In E. Carayannis, D. Campbell, & M. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense* (pp. 319-335). Springer. https://doi.org/10.1007/978-1-4939-1028-1_13

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cybersecurity culture: Current practices and future needs. *Computers & Security, 109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security, 38*(7), 97–102. https://doi.org/10.1016/j.cose.2013.04.004

White, J. K. (2017). *Impact of protection motivation theory and general deterrence theory on the behavioral intention to implement and misuse active cyber defense* (Publication No. 10622990) [Doctoral dissertation, Capella University]. ProQuest Dissertations and Theses Global